

Praxisband: Kontrollkatalog, Formularbuch und Fallstudien

Arbeitsunterlagen zu den sechs Fachleitfäden Cyber-Physical AI Security

60 prüfbare Anforderungen, 16 ausfüllbare Formulare und drei durchgängige, ausdrücklich konstruierte Fallstudien für die lokale Anwendung der sechs Fachleitfäden.

Fassung 1.0 · Stand 25. September 2026 · Adressaten: Fachprüfer, Sicherheitsarchitekten, Qualitätsverantwortliche und Verantwortliche für die lokale Einführung der Leitfäden.

Dokumenttyp: Arbeitsunterlagen-Band. Alle lokalen Bewertungen im Kontrollkatalog stehen auf NICHT ERHOBEN; die Formulare sind Vorlagen, keine bereits erhobenen Betriebsnachweise; die drei Fallstudien sind ausdrücklich konstruierte Lehr- und Prüfbeispiele, keine beobachteten Vorfälle oder ausgeführten Tests.

Steckbrief

Merkmal	Wert
Dokumenttyp	Arbeitsunterlagen-Band; keine erhobenen Betriebsdaten, keine ausgeführten Tests
Zielgruppe	Fachprüfer, Sicherheitsarchitekten, Qualitätsverantwortliche
Recherche- und Rechtsstand	25. September 2026
Umfang	13.428 Wörter, 46 Seiten
Belege	0 Literatureinträge, 0 Quellenadressen
Gliederung	84 nummerierte Abschnitte, 16 Tabellen

Inhalt

Kontrollkatalog · 60 prüfbare Anforderungen	7
Verwendung	7
K01 · Leistungs- und Systemgrenze	7
K02 · Verifizierte Daten- und Diensteflüsse	7
K03 · Gemeinsame Ursachen und Vertrauensanker	8
K04 · Wirkungsketten statt Schlagworte	8
K05 · Fachentscheidung und Vertretung	8
K06 · Nachweisfall mit Gegenbelegsuche	9
K07 · Quellen- und Rechtsstand	9
K08 · Betriebsmodi und Abbruchbedingungen	10
K09 · Patienten- und Aufenthaltsidentität	10
K10 · Trennung klinischer Vorschläge und Freigaben	10
K11 · Labor-Ende-zu-Ende-Nachweis	11
K12 · Bildgebung und Befundversionen	11
K13 · Herkunft und Unsicherheit klinischer KI-Ausgaben	12
K14 · Klinische Datenflüsse einschließlich KI-Nebendiensten	12
K15 · Gerätefunktion ohne zentrale Vernetzung	12
K16 · Klinische Ersatzkommunikation und Schichtwechsel	13
K17 · Tragfähigkeit der klinischen Mindestversorgung	13
K18 · Klinischer Ereignisabgleich	13
K19 · Freigegebene Programme und Parameter	14
K20 · Unabhängigkeit erforderlicher Schutzfunktionen	14
K21 · Zonen und fachlich erlaubte Übergänge	15
K22 · Auftragsbezogene Fernwartung	15
K23 · Qualitäts- und Chargenintegrität	15
K24 · Änderungsnachweis für Gesamtverhalten	16
K25 · Mobile Flotten und alte Aufträge	16
K26 · Sicherer Stillstand ist anlagenbezogen	16
K27 · Begrenzte Vernetzung von Altanlagen	17
K28 · Physischer Zustand beim Wiederanlauf	17
K29 · Eigene Agentenidentität	18
K30 · Eng definierte Werkzeugrechte	18
K31 · Nicht verstärkende Unterdelegation	18
K32 · Unabhängige Kontextquelle	19
K33 · Daten werden nicht zu Berechtigungen	19
K34 · Begrenzte Ausleitung und sichere Protokolle	19
K35 · Widerruf bis zum Endpunkt	20

K36 · Zustandsbindung und Wiederholungsaufträge	20
K37 · Fehlerverhalten der Kontrollschicht	20
K38 · Begrenzte defensive Autonomie	21
K39 · Begründete Rechtsrollen	21
K40 · Leitungsmandat und Risikoakzeptanz	22
K41 · Interdisziplinäre Entscheidung ohne Schattenorgan	22
K42 · Beschaffung mit Abnahmebedingungen	22
K43 · Lieferantenänderung und Ausstieg	23
K44 · Getrennte Meldespuren	23
K45 · Datenschutz und Beschäftigtenrechte im Monitoring	23
K46 · Befristete Ausnahmen	24
K47 · Kompetenz und ausreichende Vertretung	24
K48 · Berichte mit Nachweisqualität statt Gesamtscore	25
K49 · Genehmigter Prüfumfang	25
K50 · Positive und negative Testfälle	25
K51 · Zeitmessung bis zur Wirkung	26
K52 · Validierter Referenzzustand	26
K53 · Getrennte und erprobte Wiederherstellungsressourcen	26
K54 · Recovery-Bootstrap ohne Zirkelschluss	27
K55 · Nachvollziehbare Evidenzsicherung	27
K56 · Eingrenzung mit Betriebsfolgen	27
K57 · Getrennte Lage- und Meldekommunikation	28
K58 · Vollprozessübung mit Ressourcen	28
K59 · Abgleich realer und digitaler Ereignisse	29
K60 · Gestufte Wiederfreigabe und Nachprüfung	29

Formularbuch · F01 bis F16 **29**

Ausfüllbare Arbeitsunterlagen für lokale Analyse, Prüfung und Freigabe	29
F01 · System- und Leistungssteckbrief	30
F02 · Abhängigkeits- und Datenflussregister	30
F03 · Register der Handlungsvollmachten	31
F04 · Risiko- und Gefährdungsfall	31
F05 · Begründeter Nachweisfall	32
F06 · Rollen, Rechtsanwendbarkeit und Zuständigkeiten	32
F07 · Änderungs- und Rollbackentscheidung	33
F08 · Betriebsmodus und sichere Mindestleistung	33
F09 · Mandat für Cyber-Eingrenzung und defensive Agenten	34
F10 · Wiederaufbau und gestufte Wiederfreigabe	35
F11 · Ereignisabgleich und Konfliktentscheidung	35
F12 · Lieferanten-, Produkt- und Vertragsnachweise	35

F13 · Incident- und Meldeentscheidungen	36
F14 · Befristete Ausnahme und Restrisiko	37
F15 · Prüf- und Übungsprotokoll	37
F16 · Ausschussentscheidung und Betriebsfreigabe	38
Drei durchgängige Fallstudien	38
Von einer plausiblen Störung zur begründeten Betriebsentscheidung	38
S-KLINIK · Die Systeme laufen, aber ein Befund ist nicht mehr eindeutig zuzuordnen	38
1. Auftrag, Systemgrenze und Annahmen	38
2. Schadenshypothese und Gegenhypothesen	39
3. Erstentscheidung und begrenzte Eingrenzung	39
4. Notbetrieb mit realer Personal- und Kommunikationsgrenze	39
5. Prüfaufbau und verlangte Evidenz	40
6. Wiederherstellung und Zusammenführung	40
7. Ausschussentscheidung und verbleibende Unsicherheit	40
S-INDUSTRIE · Der Roboter stoppt sicher, die produzierte Charge ist trotzdem zweifelhaft	40
1. Auftrag und Annahmen	40
2. Warum eine reine Safety-Betrachtung zu kurz greift	41
3. Eingrenzung nach Funktionen statt pauschalem Netzwerkbild	41
4. Die entscheidenden technischen Gegenproben	41
5. Wiederaufbau und Produktentscheidung	42
6. Mögliche Freigabe und Gegenbeleg	42
S-ABWEHR · Ein plausibler Fehlalarm darf nicht die gesamte Organisation abschalten	42
1. Auftrag und konkurrierende Risiken	42
2. Was die Erkennung wissen darf – und was nicht	42
3. Reaktionsmandat und menschliche Entscheidung	43
4. Drei Prüfungen statt einer beeindruckenden Demonstration	43
5. Ausschussentscheidung und Restrisiko	43
Gemeinsame Auswertung	43
Quellen- und Navigationshinweis	44
12 Rechtliche Hinweise	45
12.1 Keine Beratung	45
12.2 Keine Zusicherung, keine Konformitätsaussage	45
12.3 Rechtsstand	45
12.4 Haftung	45
12.5 Verweise auf fremde Inhalte	45
12.6 Marken und Produktbezeichnungen	45
12.7 Urheberrecht und Nutzung	45
12.8 Keine personenbezogenen Daten	46
12.9 Unabhängigkeit	46

12.10 Anwendbares Recht	46
-----------------------------------	----

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Praxisband: Kontrollkatalog, Formularbuch und Fallstudien*. Fassung 1.0, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus drei Markdown-Quellen des Leitfaden-Pakets zusammengesetzt und gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Gesetzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält keine Abbildungen.

Kontrollkatalog · 60 prüfbare Anforderungen

Status: Alle lokalen Bewertungen stehen auf **NICHT ERHOBEN**. Die Kontrollen sind eine eigene fachliche Synthese für die lokale Anpassung, kein behaupteter wörtlicher Pflichtenkatalog einer einzelnen Norm. Wo ein Gesetz zwingende Pflichten begründet, sind Rolle, Scope und konkrete Vorgabe gesondert zu prüfen. Eine Zuordnung zu einer Quelle bedeutet fachliche Grundlage, nicht automatisch Klauselgleichheit.

Verwendung

Für jede anwendbare Kontrolle werden Eigentümer, lokaler Scope, Nachweiskennungen, Testdatum, Ergebnis, offene Punkte und Freigabeentscheidung ergänzt. Nichtanwendbarkeit benötigt eine Begründung. Fehlende Evidenz darf weder als bestanden noch als automatisch sicherheitswidrig umetikettiert werden; sie begrenzt den Nachweis und kann die betroffene Freigabe sperren. Akzeptanzkriterien sind vor der Prüfung zu konkretisieren, nicht nachträglich an ein gewünschtes Ergebnis anzupassen.

Ergebniszustände: nicht erhoben; erfüllt; teilweise erfüllt; nicht erfüllt; nicht anwendbar mit Begründung.

Evidenztiefe: dokumentiert; im Test beobachtet; fachlich validiert; im genehmigten Betrieb wiederkehrend bestätigt. Diese Achsen bleiben getrennt.

K01 · Leistungs- und Systemgrenze

Anwendung: Alle. **Verantwortung:** Fachlicher Leistungs- und Systemeigentümer.

Problem: Ein technisches Teilsystem wird freigegeben, obwohl die relevante klinische oder industrielle Leistung außerhalb des Tests liegt.

Anforderung / Umsetzung: Den freizugebenden Nutzungsumfang über Leistung, Beteiligte, Daten, Schnittstellen, Betriebsarten und ausdrücklich ausgeschlossene Funktionen beschreiben.

Erwarteter Nachweis: F01 mit Systemstand, Funktionsgrenze und unterschriebener Scope-Entscheidung.

Positivtest: Einen vorgesehenen Vorgang vollständig der Systembeschreibung zuordnen.

Negativ- oder Grenztest: Einen nicht vorgesehenen Schreib- oder Steuerpfad vorstellen und seine Behandlung prüfen.

Abnahmekriterium: Alle für den freigegebenen Vorgang notwendigen Komponenten und Entscheidungspunkte sind zugeordnet; Ausschlüsse sind nachvollziehbar.

Aussagegrenze / Restrisiko: Ein Scope kann unbekannte Schattenprozesse übersehen; Rückmeldungen und Änderungsabgleich bleiben erforderlich.

Grundlagen: [Q02; Q04]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K02 · Verifizierte Daten- und Diensteflüsse

Anwendung: Alle. **Verantwortung:** Architektur mit Fachbetrieb.

Problem: Undokumentierte Übertragung oder technische Abhängigkeit umgeht die vorgesehenen Kontrollen.

Anforderung / Umsetzung: Flüsse mit Quelle, Ziel, Zweck, Datenobjekt, Operation, Eigentümer und Ausfallwirkung erfassen und gegen Konfiguration beziehungsweise genehmigte Beobachtung abgleichen.

Erwarteter Nachweis: F02, Netz-/Schnittstellenplan, API-Inventar und dokumentierter Konfigurationsabgleich.

Positivtest: Einen regulären Ende-zu-Ende-Vorgang in Inventar und Beobachtung wiederfinden.

Negativ- oder Grenztest: Eine im Vertrag erwähnte, im Diagramm fehlende Herstellerverbindung als Prüfabweichung behandeln.

Abnahmekriterium: Unterschiede zwischen Dokumentation und geprüfter Konfiguration sind geklärt oder als nicht freigegebener Pfad gesperrt.

Aussagegrenze / Restrisiko: Passive Beobachtung deckt seltene oder nur im Ausfall aktive Verbindungen nicht vollständig ab.

Grundlagen: [Q02; Q16]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K03 · Gemeinsame Ursachen und Vertrauensanker

Anwendung: Alle. **Verantwortung:** Sicherheitsarchitektur mit Betriebs- und Safety-Verantwortung.

Problem: Betrieb, Schutz, Protokolle und Recovery hängen vom selben kompromittierbaren Dienst ab.

Anforderung / Umsetzung: Identität, Management, Zeit, Strom, Updates, Schlüssel und Backupzugang auf gemeinsame Ausfall- oder Kompromittierungsursachen analysieren.

Erwarteter Nachweis: Abhängigkeitsgraph mit markierten gemeinsamen Ursachen und begründeten Schutzannahmen.

Positivtest: Verbleibende Funktionen bei einem definierten gemeinsamen Dienstausfall nachvollziehbar nachweisen.

Negativ- oder Grenztest: Annehmen, dass das gemeinsame Administrationskonto kompromittiert ist; Reichweite der Wirkung bestimmen.

Abnahmekriterium: Für jeden kritischen gemeinsamen Pfad existiert eine begründete Begrenzung oder eine dokumentierte Nutzungssperre.

Aussagegrenze / Restrisiko: Unabhängige Produkte können gemeinsame Komponenten oder Dienstleister besitzen.

Grundlagen: [Q02; Q07]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K04 · Wirkungsketten statt Schlagworte

Anwendung: Alle. **Verantwortung:** Fachliches Risikomanagement.

Problem: Unspezifische Risikolisten führen zu Kontrollen ohne belegbaren Bezug zum möglichen Schaden.

Anforderung / Umsetzung: Verlust, Gefährdungszustand, Akteur/Fehler, Zugriffsweg, Handlung, Barriere und offene Annahme pro wesentlichem Szenario dokumentieren.

Erwarteter Nachweis: F04 mit Szenarien und Verknüpfung zu Kontrollkennungen.

Positivtest: Für einen Verlust jeden notwendigen Übergang und seine Barriere erläutern.

Negativ- oder Grenztest: Einen nicht böswilligen Fehler mit derselben Wirkung betrachten.

Abnahmekriterium: Kritische Verlustszenarien besitzen konkrete Pfade und passende Kontrollen; unbelegte Häufigkeiten werden nicht als Zahlen verwendet.

Aussagegrenze / Restrisiko: Die Analyse ist nicht automatisch vollständig; Änderungen und Ereignisse können neue Pfade offenlegen.

Grundlagen: [Q02; Q11]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K05 · Fachentscheidung und Vertretung

Anwendung: Alle. **Verantwortung:** Leitung.

Problem: Eine technische Stelle trifft unbefugt eine klinische oder Safety-relevante Entscheidung, oder niemand ist erreichbar.

Anforderung / Umsetzung: Entscheidungstypen, Kompetenz, Mandat, Vertretung und Eskalation im Normalbetrieb und in der Krise festlegen.

Erwarteter Nachweis: F06 Rollenblatt und Vertretungsnachweis; genehmigtes Reaktionsmandat.

Positivtest: Eine entscheidungsbefugte Vertretung in einer vereinbarten Übung erreichen.

Negativ- oder Grenztest: Den Ausfall der regulären Schlüsselperson simulieren.

Abnahmekriterium: Für jede kritische Entscheidung existiert eine tatsächlich nutzbare Zuständigkeit mit benötigter Fachbeteiligung.

Aussagegrenze / Restrisiko: Formale Benennung ersetzt weder ausreichende Kapazität noch tatsächliche Entscheidungsfähigkeit.

Grundlagen: [Q04; Q29]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K06 · Nachweisfall mit Gegenbelegsuche

Anwendung: Alle. **Verantwortung:** Unabhängige Prüfverantwortung.

Problem: Eine Freigabe beruht nur auf Absichtserklärungen oder selektiv positiven Tests.

Anforderung / Umsetzung: Behauptung, Argument, Evidenz, Gegenprobe, Grenzen und Gültigkeitsbedingungen je kritischer Freigabe verbinden.

Erwarteter Nachweis: F05 und referenzierte E-/P-Nachweise.

Positivtest: Eine Sicherheitsbehauptung aus den verknüpften Belegen rekonstruieren.

Negativ- oder Grenztest: Einen alternativen Zugriffspfad oder eine abweichende Systemversion gegen die Behauptung prüfen.

Abnahmekriterium: Aussageumfang entspricht dem tatsächlichen Nachweis; Gegenbelege sind nicht durch Mittelwerte verdeckt.

Aussagegrenze / Restrisiko: Endliche Tests beweisen nicht die Abwesenheit aller unbekannten Schwächen.

Grundlagen: [Q07; Q05]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K07 · Quellen- und Rechtsstand

Anwendung: Alle. **Verantwortung:** Recht/Compliance und fachlicher Dokumenteneigentümer.

Problem: Ein Entwurf oder eine veraltete Frist wird als verbindlicher aktueller Maßstab verwendet.

Anforderung / Umsetzung: Externe Grundlage mit Ausgabe, Status, Fundstelle, Anwendungsbereich und tatsächlicher Zugriffstiefe dokumentieren.

Erwarteter Nachweis: Q-Register und lokaler Rechts-/Normencheck F06.

Positivtest: Eine tragende Aussage bis zum passenden Absatz beziehungsweise Quellenabschnitt zurückverfolgen.

Negativ- oder Grenztest: Ein Normabstract als angeblichen Detail-Konformitätsnachweis vorlegen und zurückweisen.

Abnahmekriterium: Pflichten, Leitlinien, Entwürfe und eigene Empfehlungen sind unterscheidbar; kritische offene Rechtsfragen verhindern eine uneingeschränkte lokale Freigabe.

Aussagegrenze / Restrisiko: Zwischen Abruf und Anwendung können Änderungen eintreten.

Grundlagen: [Q03; Q33; Q29]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K08 · Betriebsmodi und Abbruchbedingungen

Anwendung: Alle. **Verantwortung:** Fachlicher Betrieb.

Problem: Ein Ersatzmodus ist verfügbar, wird aber zu lange oder unter ungeeigneten Bedingungen genutzt.

Anforderung / Umsetzung: Für jeden zulässigen Modus erhaltene/verlorene Funktionen, Ressourcen, Eintritt, Überwachung, zulässige Dauer und Austritt festlegen.

Erwarteter Nachweis: F08 und genehmigte Übungsprotokolle.

Positivtest: Einen genehmigten Modus samt Ressourcennachweis nachvollziehbar aktivieren.

Negativ- oder Grenztest: Eine notwendige Ressource als erschöpft annehmen und die Eskalation prüfen.

Abnahmekriterium: Eintritt und Ende der Vertretbarkeit sind erkennbar; eine geeignete Alternative oder Einschränkung ist vorgesehen.

Aussagegrenze / Restrisiko: Dauergrenzen sind lokal fachlich festzulegen, nicht aus diesem Leitfaden zu übernehmen.

Grundlagen: [Q02; Q18]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K09 · Patienten- und Aufenthaltsidentität

Anwendung: Klinik. **Verantwortung:** Klinischer Prozessverantwortlicher mit Aufnahme/Labor.

Problem: Ein richtiger Befund oder Auftrag wird einer falschen Person zugeordnet.

Anforderung / Umsetzung: Identität über Aufnahme, Auftrag, Probe, Befund und Ersatzdokumentation verbinden; Konflikt- und Zusammenführungsverfahren festlegen.

Erwarteter Nachweis: F01/F11 und freigegebenes Identitätsverfahren.

Positivtest: Einen synthetischen Patienten durch den vollständigen Ersatz- und Rückkehrprozess führen.

Negativ- oder Grenztest: Eine doppelte oder widersprüchliche Ersatzidentität einspielen.

Abnahmekriterium: Konflikt wird erkannt und fachlich entschieden; keine stille automatische Zusammenführung kritischer Angaben.

Aussagegrenze / Restrisiko: Technische Zuordnung allein beweist nicht die Richtigkeit ursprünglicher menschlicher Erfassung.

Grundlagen: [Q16; Q18]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K10 · Trennung klinischer Vorschläge und Freigaben

Anwendung: Klinik. **Verantwortung:** Klinische Leitung und zuständige Fachbereiche.

Problem: Ein KI-Entwurf wird ohne vorgesehene fachliche Entscheidung als verbindlicher Auftrag wirksam.

Anforderung / Umsetzung: Entwurf, Verordnung/Auftrag, Ausführung und Dokumentation mit getrennten Berechtigungen und Statusübergängen führen.

Erwarteter Nachweis: Berechtigungsmodell, Statusmodell, F03 und F15.

Positivtest: Einen freigegebenen synthetischen Vorgang mit sichtbaren Rollenübergängen durchführen.

Negativ- oder Grenztest: Der Entwurfsagent versucht den fachlichen Freigabestatus selbst zu setzen.

Abnahmekriterium: Der unzulässige Übergang wird an der ausführenden Schnittstelle verhindert; zulässiger Ablauf bleibt möglich.

Aussagegrenze / Restrisiko: Fachliche Bewertung der Inhalte wird nicht durch die technische Rollentrennung ersetzt.

Grundlagen: [Q16; Q22]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K11 · Labor-Ende-zu-Ende-Nachweis

Anwendung: Klinik/Labor. **Verantwortung:** Laborleitung mit klinischem Empfänger.

Problem: Ein erzeugtes Ergebnis erreicht den richtigen klinischen Empfänger nicht oder in falscher Version.

Anforderung / Umsetzung: Auftrag, Probe, Freigabe, Übermittlung, Korrektur und Empfang im Normal- und Ersatzprozess verbinden.

Erwarteter Nachweis: Labor-Ersatzprozess, Empfangsnachweise und synthetischer Falltest.

Positivtest: Auftrag und Ergebnis einschließlich Korrekturstand korrekt zuordnen.

Negativ- oder Grenztest: Eine doppelte beziehungsweise verspätete Übertragung im Test anbieten.

Abnahmekriterium: Verwechslung wird verhindert oder sichtbar geklärt; fachlich festgelegte zeitliche Anforderungen werden nachgewiesen.

Aussagegrenze / Restrisiko: Keine allgemeinen klinischen Zeitgrenzen; Test muss lokale Betriebsbedingungen berücksichtigen.

Grundlagen: [Q18; Q21]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K12 · Bildgebung und Befundversionen

Anwendung: Klinik/Radiologie. **Verantwortung:** Radiologie mit IT-Integration.

Problem: Veraltete oder falsch zugeordnete Bild-/Befundinformationen erscheinen als aktuelle Grundlage.

Anforderung / Umsetzung: Patientenbezug, Untersuchungszeit, Serie, Vorbefund und Freigabestand für relevante Prozesse eindeutig halten.

Erwarteter Nachweis: Schnittstellenbeschreibung und fachlich bewertete Testfälle.

Positivtest: Ein synthetischer Korrekturbefund wird mit dem richtigen Untersuchungsstand angezeigt.

Negativ- oder Grenztest: Eine unvollständige oder widersprüchliche Serie zur automatischen Weiterverarbeitung anbieten.

Abnahmekriterium: Ungeeignete Grundlage wird sichtbar und nach dem freigegebenen Verfahren behandelt.

Aussagegrenze / Restrisiko: Formale Datenvalidität belegt nicht die diagnostische Eignung.

Grundlagen: [Q16; Q22]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K13 · Herkunft und Unsicherheit klinischer KI-Ausgaben

Anwendung: Klinik/KI. **Verantwortung:** Klinischer Anwendungseigentümer.

Problem: Eine KI formuliert unsichere Daten in scheinbar eindeutige Aussagen um.

Anforderung / Umsetzung: Eingangsquelle, Version und relevante Unsicherheit erreichbar halten; automatische Übernahme bei unzulässiger Grundlage begrenzen.

Erwarteter Nachweis: Freigabekriterien, Darstellungsnachweis und Testdatensatz ohne Patientendaten.

Positivtest: Eine freigegebene Ausgabe bis zu ihren verwendeten Daten zurückverfolgen.

Negativ- oder Grenztest: Eine als ungeklärt markierte Quelle in den Testfall aufnehmen.

Abnahmekriterium: Unsicherheit bleibt sichtbar; nicht freigegebene automatische Wirkung wird verhindert.

Aussagegrenze / Restrisiko: Nachvollziehbare Herkunft ist kein Beweis medizinischer Richtigkeit.

Grundlagen: [Q11; Q12; Q16]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K14 · Klinische Datenflüsse einschließlich KI-Nebendiensten

Anwendung: Klinik/Datenschutz. **Verantwortung:** Verantwortlicher mit Datenschutzberatung und IT.

Problem: Patienteninformationen gelangen in nicht erfasste Modell-, Protokoll- oder Supportdienste.

Anforderung / Umsetzung: Eingaben, Ausgaben, Speicher, Suchindizes, Diagnosedaten und externe Empfänger tatsächlich inventarisieren und zweckbezogen beschränken.

Erwarteter Nachweis: Verarbeitungskarte, F02, Verträge und technische Empfängerliste.

Positivtest: Einen Testvorgang über alle erfassten Dienste verfolgen.

Negativ- oder Grenztest: Einen ungeplanten externen Empfänger oder erweiterten Datenumfang anfordern.

Abnahmekriterium: Nicht zugelassene Weitergabe wird verhindert oder vor Wirksamkeit gestoppt; Rechtsgrundlage und Zweck sind lokal geprüft.

Aussagegrenze / Restrisiko: Vertragsaussagen allein beweisen keinen vollständigen technischen Datenfluss.

Grundlagen: [Q16; Q38]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K15 · Gerätefunktion ohne zentrale Vernetzung

Anwendung: Klinik/Medizintechnik. **Verantwortung:** Medizintechnik und klinische Leitung.

Problem: Lokale Anzeige bleibt bestehen, aber die notwendige Alarm-/Überwachungskette fällt aus.

Anforderung / Umsetzung: Pro Gerätetyp Netzwerk, Alarmierung, lokale Anzeige, Dokumentation und Personaleinsatz getrennt beurteilen.

Erwarteter Nachweis: Herstellerdokumentation, Modusmatrix und genehmigte funktionsbezogene Prüfung.

Positivtest: Den dokumentierten Ersatzmodus unter sicheren Testbedingungen nachweisen.

Negativ- oder Grenztest: Zentrale Alarmweiterleitung als ausgefallen annehmen und notwendige Kompensation prüfen.

Abnahmekriterium: Erhaltene und verlorene Funktionen sind fachlich bewertet; erforderliche Ersatzressourcen sind verfügbar.

Aussagegrenze / Restrisiko: Kein allgemeiner Auftrag zur Netztrennung; Modell- und Verwendungsscope bleiben entscheidend.

Grundlagen: [Q19; Q23]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K16 · Klinische Ersatzkommunikation und Schichtwechsel

Anwendung: Klinik. **Verantwortung:** Klinische Betriebs-/Notfallkoordination.

Problem: Ein Verfahren funktioniert nur mit dem Wissen einer Person oder über die ausgefallene Haupt-IT.

Anforderung / Umsetzung: Erreichbarkeit, unabhängige Kommunikationsmittel, Übergabe und Vertretung unter realistischen Besetzungsannahmen vorbereiten.

Erwarteter Nachweis: Kommunikationsplan, aktuelle Offlinekontakte und Übergabetest.

Positivtest: Im Übungsszenario einen vollständigen Schichtwechsel mit offenen Vorgängen durchführen.

Negativ- oder Grenztest: Haupttelefonie und zentrale Anmeldung als nicht verfügbar annehmen.

Abnahmekriterium: Lage, offene Aufgaben und Entscheidungen bleiben über den Wechsel hinweg nachvollziehbar.

Aussagegrenze / Restrisiko: Reservewege können gemeinsame Strom- oder Netzdienste nutzen; Unabhängigkeit prüfen.

Grundlagen: [Q18; Q17]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K17 · Tragfähigkeit der klinischen Mindestversorgung

Anwendung: Klinik. **Verantwortung:** Klinische Leitung mit Pflege und Betrieb.

Problem: Ein Papierplan überschätzt Dauer, Personal oder Material des Ersatzbetriebs.

Anforderung / Umsetzung: Priorisierte Leistungen mit Ressourcenbedarf, zeitlicher Grenze und regionaler Abstimmung definieren.

Erwarteter Nachweis: F08, Ressourcenliste und Vollprozessübung.

Positivtest: Einen genehmigten Ersatzprozess einschließlich Material- und Personalannahmen durchführen.

Negativ- oder Grenztest: Eine definierte zusätzliche Belastung oder Ressourcengrenze in der Übung einspielen.

Abnahmekriterium: Grenze der vertretbaren Leistung wird erkannt und an eine entscheidungsbefugte Stelle eskaliert.

Aussagegrenze / Restrisiko: Regionale Alternativkapazität ist nicht garantiert und muss abgestimmt werden.

Grundlagen: [Q18; Q20]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K18 · Klinischer Ereignisabgleich

Anwendung: Klinik/Recovery. **Verantwortung:** Klinischer Daten-/Prozesseigentümer.

Problem: Nach Restore werden erledigte Vorgänge erneut ausgelöst oder manuelle Informationen falsch zugeordnet.

Anforderung / Umsetzung: Ereigniszeit, Erfassungszeit, Urheber, Patientenbezug, Dubletten und fachliche Konfliktentscheidung getrennt führen.

Erwarteter Nachweis: F11 mit abgearbeiteten synthetischen Konfliktfällen.

Positivtest: Ersatzdokumentation verlustfrei und mit Herkunft in den Testbestand übernehmen.

Negativ- oder Grenztest: Einen bereits erledigten Auftrag und einen widersprüchlichen Eintrag anbieten.

Abnahmekriterium: Keine unkontrollierte Doppelausführung; kritische Konflikte sind vor entscheidungsrelevanter Verwendung geklärt.

Aussagegrenze / Restrisiko: Nicht alle Inhalte können sofort geprüft werden; verbleibende Unsicherheit muss sichtbar begrenzt werden.

Grundlagen: [Q18; Q16]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K19 · Freigegebene Programme und Parameter

Anwendung: Industrie. **Verantwortung:** OT/Engineering mit Produktion.

Problem: Eine digitale Änderung verändert den Prozess außerhalb des genehmigten Zustands.

Anforderung / Umsetzung: Programm-, Rezept-, Parameter- und Konfigurationsstände versionieren, berechtigen und dem Auftrag zuordnen.

Erwarteter Nachweis: Konfigurationsbaseline, Änderungsprotokoll und F07.

Positivtest: Einen genehmigten Wechsel vollständig bis zur verwendeten Version verfolgen.

Negativ- oder Grenztest: Eine nicht freigegebene Änderung über einen Hilfszugang versuchen.

Abnahmekriterium: Unzulässige Änderung wird verhindert oder vor Nutzung erkannt; genutzter Stand ist nachweisbar.

Aussagegrenze / Restrisiko: Signatur und Version bestätigen nicht die fachliche Eignung des Parameters.

Grundlagen: [Q02; Q24]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K20 · Unabhängigkeit erforderlicher Schutzfunktionen

Anwendung: Industrie/Safety. **Verantwortung:** Funktionale Sicherheit mit Anlagenverantwortung.

Problem: Kompromittierte operative Rechte verändern gleichzeitig die letzte Begrenzung gefährlicher Wirkung.

Anforderung / Umsetzung: Schutzfunktionen, Änderungswege und gemeinsame Ursachen anlagenbezogen analysieren und geeignet absichern.

Erwarteter Nachweis: Schutzfunktionsnachweis, Berechtigungs- und Managementpfadanalyse.

Positivtest: Wirksamkeit der erforderlichen Schutzfunktion im genehmigten Prüfverfahren bestätigen.

Negativ- oder Grenztest: Kompromittierung der operativen Agenten-/Managementidentität im Modell annehmen.

Abnahmekriterium: Die kritische Schutzbehauptung bleibt unter den festgelegten Annahmen begründet; unbekannte letzte Grenzen sperren die neue Funktion.

Aussagegrenze / Restrisiko: Kein pauschaler Safety-Level; einschlägige Normen und reale Integration sind separat zu prüfen.

Grundlagen: [Q02; Q27; Q28]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K21 · Zonen und fachlich erlaubte Übergänge

Anwendung: Industrie/OT. **Verantwortung:** OT-Sicherheitsarchitektur.

Problem: Eine formale Netztrennung wird durch geteilte Konten oder Wartungspfade umgangen.

Anforderung / Umsetzung: Zonen mit Schutzbedarf und Kommunikationspfade mit Zweck, Operation und Ausfallverhalten festlegen.

Erwarteter Nachweis: Zonen-/Conduit-Modell, Regeln und geprüfte Zugriffsmatrix.

Positivtest: Einen notwendigen Übergang im freigegebenen Funktionsumfang nachweisen.

Negativ- oder Grenztest: Einen Zugriff aus einer nicht zugelassenen Zone über einen alternativen Pfad prüfen.

Abnahmekriterium: Erlaubte Funktion bleibt erhalten; nicht erlaubte Pfade sind nachweislich begrenzt.

Aussagegrenze / Restrisiko: Netzzonen allein verhindern keinen missbräuchlichen fachlichen Befehl innerhalb einer erlaubten Verbindung.

Grundlagen: [Q24; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K22 · Auftragsbezogene Fernwartung

Anwendung: Industrie/Service. **Verantwortung:** Instandhaltung/OT mit Dienstleistersteuerung.

Problem: Dauerhafte breite Herstellerrechte bleiben unkontrolliert aktiv.

Anforderung / Umsetzung: Serviceidentität, Ziel, Zeit, erlaubte Änderung, lokalen Ansprechpartner und Sitzungsabschluss festlegen.

Erwarteter Nachweis: Wartungsmandat, F03/F07, Sitzungs- und Änderungsnachweise.

Positivtest: Genehmigte Diagnose in der vereinbarten Zeit durchführen und abschließen.

Negativ- oder Grenztest: Dieselbe Identität nach Ablauf oder an einem anderen Ziel verwenden.

Abnahmekriterium: Unzulässiger Zugriff wird verhindert; verbleibende Konten, Tokens und Änderungen sind geprüft.

Aussagegrenze / Restrisiko: Widerruf am Zugang beendet nicht automatisch bereits laufende lokale Prozesse.

Grundlagen: [Q02; Q15]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K23 · Qualitäts- und Chargenintegrität

Anwendung: Industrie/Qualität. **Verantwortung:** Qualitätsleitung mit Produktion.

Problem: Produktion läuft weiter, obwohl Prüfgrenzen, Rezept oder Produktzuordnung verändert wurden.

Anforderung / Umsetzung: Kritische Produktmerkmale mit freigegebenem Prozessstand und Rückverfolgbarkeit verbinden.

Erwarteter Nachweis: Chargen-/Parameterzuordnung, Prüfstatus und Abweichungsentscheidung.

Positivtest: Ein Produktlos zu Material, Parametern, Softwarestand und Prüfung zurückverfolgen.

Negativ- oder Grenztest: Einen unklaren Parameterzeitraum in der Übung als Verdacht einführen.

Abnahmekriterium: Betroffene Produkte werden fachlich abgegrenzt und ohne ungeprüfte Freigabe behandelt.

Aussagegrenze / Restrisiko: Technische Verfügbarkeit beweist keine Qualität; zusätzliche Prüfungen können erforderlich sein.

Grundlagen: [Q02; Q31]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K24 · Änderungsnachweis für Gesamtverhalten

Anwendung: Industrie/KI. **Verantwortung:** Engineering-/Anwendungseigentümer.

Problem: Ein Werkzeug- oder Modellupdate erweitert unbemerkt die Wirkung.

Anforderung / Umsetzung: Modell, Werkzeuge, Rechte, Parameter, Integrationsschema und Rollback gemeinsam in den Freigabestand aufnehmen.

Erwarteter Nachweis: F07, Versionen und gezielte Regressionstests.

Positivtest: Eine genehmigte Änderung mit passender Nachprüfung ausrollen.

Negativ- oder Grenztest: Eine neue Schreibfähigkeit ohne erweitertes Mandat im Test aktivieren.

Abnahmekriterium: Freigabe erfasst alle wirkungsrelevanten Änderungen; alte Argumente werden bei verändertem Pfad neu bewertet.

Aussagegrenze / Restrisiko: Ein Rollback kann an Daten-/Schemaänderungen scheitern; seine Reichweite ist separat nachzuweisen.

Grundlagen: [Q02; Q12]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K25 · Mobile Flotten und alte Aufträge

Anwendung: Industrie/Logistikrobotik. **Verantwortung:** Flotten-/Robotikintegration mit Betrieb.

Problem: Alte Missionsbefehle werden nach Wiederverbindung in geändertem Umfeld wirksam.

Anforderung / Umsetzung: Flottenauftrag, lokalen Zustand, Karten-/Zonenstand, Unterbrechung und Wiederannahme von Missionen definieren.

Erwarteter Nachweis: Missionszustandsmodell und genehmigter Simulationstest.

Positivtest: Unterbrechung und geordnete Wiederaufnahme eines zulässigen Testauftrags zeigen.

Negativ- oder Grenztest: Einen alten Auftrag nach Moduswechsel erneut zustellen.

Abnahmekriterium: Kein ungeprüfter Auftrag wird in einem unzulässigen Zustand ausgeführt; lokale Schutzfunktionen bleiben gesondert wirksam.

Aussagegrenze / Restrisiko: Kollisionsbegrenzung allein schützt nicht vor blockierten Wegen und Versorgungs-/Produktionsausfall.

Grundlagen: [Q02; Q26]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K26 · Sicherer Stillstand ist anlagenbezogen

Anwendung: Industrie. **Verantwortung:** Anlagenbetrieb und Safety-Verantwortung.

Problem: Eine universelle Abschaltung beseitigt nötige Energiehaltung, Medien oder kontrollierten Nachlauf.

Anforderung / Umsetzung: Zulässige Stopp-/Mindestbetriebszustände aus Prozess und Gefährdung ableiten; Cybermaßnahmen darauf abbilden.

Erwarteter Nachweis: F08 und anlagenspezifische Schutz-/Betriebsdokumentation.

Positivtest: Genehmigten Übergang im geeigneten Prüfverfahren nachvollziehen.

Negativ- oder Grenztest: Sofortigen Energieverlust als analytischen Gegenfall betrachten, ohne ihn unkontrolliert auszulösen.

Abnahmekriterium: Not-Halt, Stopp, Energieabschaltung und Cyber-Eingrenzung sind fachlich unterschieden.

Aussagegrenze / Restrisiko: Kein universelles Abschaltschema; reale Versuche nur unter abgesicherten Bedingungen.

Grundlagen: [Q02; Q31]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K27 · Begrenzte Vernetzung von Altanlagen

Anwendung: Industrie/Brownfield. **Verantwortung:** OT/Engineering und Leitung.

Problem: Fehlende moderne Sicherheitsfunktionen werden durch neue Erreichbarkeit überfordert.

Anforderung / Umsetzung: Nicht verfügbare Schutzfunktionen offen erfassen und kompensierende Maßnahmen oder Nutzungsgrenzen festlegen.

Erwarteter Nachweis: Ausnahmeregister F14 mit Ablöse-/Überprüfungsplan.

Positivtest: Erlaubten Altanlagenzugang über den begrenzten Pfad prüfen.

Negativ- oder Grenztest: Eine im Altgerät nicht begrenzbare zusätzliche Agentenfunktion zur Freigabe vorstellen.

Abnahmekriterium: Keine neue kritische Vollmacht ohne ausreichende Begrenzung; Ausnahme hat Eigentümer und Ende.

Aussagegrenze / Restrisiko: Kompensation ist nicht automatisch gleichwertig mit einer fehlenden geräteseitigen Schutzfunktion.

Grundlagen: [Q02; Q31]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K28 · Physischer Zustand beim Wiederanlauf

Anwendung: Industrie/Recovery. **Verantwortung:** Produktion, Instandhaltung und Qualität.

Problem: Restore setzt einen digitalen Zustand voraus, der nicht zu Werkstücken, Werkzeugen oder Materialien passt.

Anforderung / Umsetzung: Realen Anlagenzustand mit Aufträgen, Material, Parametern, Schutzstatus und Qualitätslage abgleichen.

Erwarteter Nachweis: F10/F11 und fachliche Wiederanlauffreigabe.

Positivtest: Einen Testbestand nach Unterbrechung korrekt mit dem realen Modellzustand abgleichen.

Negativ- oder Grenztest: Manuelle Änderung außerhalb des digitalen Bestands in der Übung vorgeben.

Abnahmekriterium: Abweichung wird erkannt; Freigabe erfolgt erst im fachlich geklärten Umfang.

Aussagegrenze / Restrisiko: Ein digitaler Zwilling ist bei betroffenen Eingangsdaten keine unabhängige Referenz.

Grundlagen: [Q08; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K29 · Eigene Agentenidentität

Anwendung: KI/IAM. **Verantwortung:** IAM/Plattform mit Anwendungseigentümer.

Problem: Handlungen sind nur einem geteilten Konto, nicht einem Agenten und Auftrag zuzuordnen.

Anforderung / Umsetzung: Ausführende Agenten mit eigener Identität, Verantwortlichem und Auftragsbezug führen.

Erwarteter Nachweis: Agentenregister und F03.

Positivtest: Einen Vorgang bis zu Identität und Mandat rekonstruieren.

Negativ- oder Grenztest: Ein persönliches Vollzugriffstoken als dauerhaften Agentenzugang vorsehen.

Abnahmekriterium: Geteilte oder übernommene Vollrechte sind ausgeschlossen oder eng begründet und kompensiert; kritische neue Funktionen ohne Zuordnung bleiben gesperrt.

Aussagegrenze / Restrisiko: Identität beweist weder gute Absicht noch korrekte Ausführung.

Grundlagen: [Q09; Q10]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K30 · Eng definierte Werkzeugrechte

Anwendung: KI/Software. **Verantwortung:** Anwendungsentwicklung und Security.

Problem: Ein allgemeines Tool eröffnet mehr Handlungen als der fachliche Auftrag benötigt.

Anforderung / Umsetzung: Werkzeuge mit typisierten Operationen, Ressourcenscope und Feld-/Aktionsbegrenzung freigeben.

Erwarteter Nachweis: Toolkatalog, Schema und Berechtigungstests.

Positivtest: Zulässige Fachaktion mit minimalem Toolumfang durchführen.

Negativ- oder Grenztest: Zusatzfeld, fremde Ressource oder allgemeine Schreibfunktion anfordern.

Abnahmekriterium: Nicht erlaubte Aktion wird an der tatsächlichen Ausführungsgrenze verhindert.

Aussagegrenze / Restrisiko: Schema-Gültigkeit allein garantiert keine fachliche Plausibilität.

Grundlagen: [Q06; Q13]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K31 · Nicht verstärkende Unterdelegation

Anwendung: KI/IAM. **Verantwortung:** IAM-/Agentenarchitektur.

Problem: Subagenten erhalten breitere oder länger gültige Befugnisse als ihr Auftraggeber.

Anforderung / Umsetzung: Unterdelegation nach Umfang, Ziel, Tiefe, Dauer und übergeordnetem Mandat begrenzen.

Erwarteter Nachweis: Delegationsmodell und Testkette F03.

Positivtest: Zulässige Teilvollmacht an einen synthetischen Subagenten weitergeben.

Negativ- oder Grenztest: Breitere, längere oder sachfremde Vollmacht anfordern.

Abnahmekriterium: Unterdelegation erweitert die wirksame Autorität nicht und bleibt dem Auftrag zuordenbar.

Aussagegrenze / Restrisiko: Technische Delegation klärt nicht automatisch alle rechtlichen Verantwortlichkeiten.

Grundlagen: [Q14; Q09]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K32 · Unabhängige Kontextquelle

Anwendung: KI/Architektur. **Verantwortung:** Architektur mit fachlichem Prozesseigentümer.

Problem: Der Agent erklärt sich selbst zum Notfall oder verändert seinen eigenen erlaubten Kontext.

Anforderung / Umsetzung: Berechtigungsrelevante Zustände aus festgelegten vertrauenswürdigen Quellen beziehen und Aktualität prüfen.

Erwarteter Nachweis: Kontextquellenregister und Zustands-/Policytests.

Positivtest: Gültigen Kontext zur zulässigen Aktion bestätigen.

Negativ- oder Grenztest: Vom Agenten selbst behauptete Mandatserweiterung oder veralteten Zustand verwenden.

Abnahmekriterium: Unbestätigter Kontext erweitert keine Rechte; Ausfallverhalten ist funktional festgelegt.

Aussagegrenze / Restrisiko: Auch die Kontextquelle kann kompromittiert sein; Vertrauensannahmen bleiben separat zu prüfen.

Grundlagen: [Q06; Q10]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K33 · Daten werden nicht zu Berechtigungen

Anwendung: KI/Security. **Verantwortung:** KI-Engineering und Security.

Problem: Eine externe Anweisung in Dokument oder Toolantwort erweitert die ausführbaren Aktionen.

Anforderung / Umsetzung: Unvertrauenswürdige Inhalte als Daten behandeln; Rechte ausschließlich über den vorgesehenen Kontrollpfad ändern.

Erwarteter Nachweis: Synthetische Testfälle, Tool-/Policyprotokolle.

Positivtest: Unbedenklichen Inhalt für den erlaubten Zweck verarbeiten.

Negativ- oder Grenztest: Testinhalt behauptet zusätzliche Freigabe oder Aufhebung einer Regel.

Abnahmekriterium: Keine zusätzliche unzulässige Toolwirkung; Frontend-Widerspruch allein zählt nicht als Nachweis.

Aussagegrenze / Restrisiko: Nicht jeder mögliche Angriffsinhalt wird durch eine endliche Testsammlung abgedeckt.

Grundlagen: [Q11; Q06]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K34 · Begrenzte Ausleitung und sichere Protokolle

Anwendung: KI/Datenschutz. **Verantwortung:** Datenverantwortlicher mit Plattform/Security.

Problem: Leserechte erlauben indirekt umfangreichen Export oder sensible Daten landen in Logs.

Anforderung / Umsetzung: Empfänger, Datenumfang, Zweck und Protokollinhalt begrenzen; notwendige Nachweisfelder von Vollinhalten trennen.

Erwarteter Nachweis: Datenflussregeln, Loggingkonzept und Exporttests.

Positivtest: Erlaubten begrenzten Export und erforderliche Auditierung zeigen.

Negativ- oder Grenztest: Ungeplanten Empfänger oder unnötige sensible Protokollfelder anfordern.

Abnahmekriterium: Unzulässige Ausleitung verhindert; Nachweise bleiben mit zweckgerechtem Zugriff verfügbar.

Aussagegrenze / Restrisiko: Metadaten können ebenfalls sensibel sein; Rechtsprüfung bleibt erforderlich.

Grundlagen: [Q16; Q38]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K35 · Widerruf bis zum Endpunkt

Anwendung: KI/IAM. **Verantwortung:** IAM mit Zielsystemverantwortlichen.

Problem: Ein gesperrtes Token bleibt über Cache oder Session praktisch wirksam.

Anforderung / Umsetzung: Widerruf, Ablauf, Verteilung, Caches und erreichbare Endpunkte spezifizieren und messen.

Erwarteter Nachweis: Widerrufsmodell, Messprotokoll F15.

Positivtest: Zulässige Sitzung aktivieren und gezielt widerrufen.

Negativ- oder Grenztest: Nach Widerruf über bestehende Session oder getrennten Endpunkt eine neue Aktion anfordern.

Abnahmekriterium: Wirksame Begrenzung innerhalb lokal festgelegter Frist belegt; Restverhalten dokumentiert.

Aussagegrenze / Restrisiko: Laufende physische Aktionen benötigen eine eigene sichere Behandlung.

Grundlagen: [Q15; Q13]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K36 · Zustandsbindung und Wiederholungsaufträge

Anwendung: KI/Integration. **Verantwortung:** Integration und Zielsystemeigentümer.

Problem: Ein alter oder doppelt zugestellter Auftrag erzeugt eine unzulässige zweite Wirkung.

Anforderung / Umsetzung: Auftragskennung, Zustandsversion, Ablauf und Ausführungsprüfung für relevante Aktionen festlegen.

Erwarteter Nachweis: Auftragszustandsmodell und Wiederholungs-/State-tests.

Positivtest: Einen gültigen Auftrag eindeutig ausführen und bestätigen.

Negativ- oder Grenztest: Denselben Auftrag erneut oder nach Betriebsmoduswechsel anbieten.

Abnahmekriterium: Veraltete oder doppelte Wirkungen werden gemäß fachlicher Vorgabe ausgeschlossen oder sichtbar eskaliert.

Aussagegrenze / Restrisiko: API-Idempotenz ist nicht automatisch physische Idempotenz.

Grundlagen: [Q06; Q15]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K37 · Fehlerverhalten der Kontrollschicht

Anwendung: KI/OT/Klinik. **Verantwortung:** Architektur mit Fachbetrieb/Safety.

Problem: Ausfall der Policy-Engine führt entweder zu Vollzugriff oder gefährlichem Funktionsabbruch.

Anforderung / Umsetzung: Je Funktion Verhalten bei fehlender Autorisierung, Zeit, Kontext oder Logging bestimmen.

Erwarteter Nachweis: Fehlermodusmatrix und genehmigte Ausfallsimulation.

Positivtest: Erwartete eingeschränkte Funktion bei einem definierten Fehler zeigen.

Negativ- oder Grenztest: Mehrere gemeinsame Kontrollabhängigkeiten gleichzeitig als ausgefallen annehmen.

Abnahmekriterium: Keine pauschale Rechteauserweiterung; notwendige lokale Schutz-/Betriebsfunktionen bleiben nach ihrem eigenen Nachweis erhalten.

Aussagegrenze / Restrisiko: Eine universelle Fail-closed-Regel genügt nicht für jede physische Funktion.

Grundlagen: [Q02; Q06]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K38 · Begrenzte defensive Autonomie

Anwendung: SOC/KI. **Verantwortung:** SOC-Leitung mit Fachbetrieb.

Problem: Ein Fehlalarm löst eine überbreite Abschaltung kritischer Funktionen aus.

Anforderung / Umsetzung: Automatische Gegenmaßnahmen mit Scope, Wirkung, Freigabe und Rücknahme vorab mandatieren.

Erwarteter Nachweis: F09 und Fehlalarmübung.

Positivtest: Einen bestätigten Testbefund innerhalb des Mandats bearbeiten.

Negativ- oder Grenztest: Ungewöhnliche, aber legitime Wartung oder irreführende Logs anbieten.

Abnahmekriterium: Defensivagent bleibt innerhalb seiner Rechte; weitergehende Eingriffe werden nach festgelegtem Verfahren entschieden.

Aussagegrenze / Restrisiko: Detektionsunsicherheit und betriebliche Nebenwirkung bleiben Lagefragen.

Grundlagen: [Q05; Q10]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K39 · Begründete Rechtsrollen

Anwendung: Governance/Recht. **Verantwortung:** Recht/Compliance mit Leitung.

Problem: Pflichten werden einem falschen Akteur zugeordnet oder wegen eines Stichtags pauschal aufgeschoben.

Anforderung / Umsetzung: Organisation, Produkt, Betrieb, KI-Verwendung, Datenrolle und einschlägige Rechtsregime dokumentieren.

Erwarteter Nachweis: F06 mit aktuellem Quellenstand und offenen Subsumtionspunkten.

Positivtest: Eine konkrete Anwendung durch alle relevanten Rollenprüfungen führen.

Negativ- oder Grenztest: Scopeänderung oder neue Produktweitergabe als Gegenfall einspielen.

Abnahmekriterium: Anwendbarkeit ist begründet; offene entscheidende Rechtsfragen sind ausdrücklich Freigabevorbehalte.

Aussagegrenze / Restrisiko: Dieser Leitfaden ist keine individuelle Rechtsberatung oder abschließendes Rechtskataster.

Grundlagen: [Q29; Q30; Q33; Q36]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K40 · Leitungsmandat und Risikoakzeptanz

Anwendung: Governance. **Verantwortung:** Geschäfts-/Klinik-/Werkleitung.

Problem: Risiken werden informell vom Projektteam akzeptiert, obwohl dieses nicht entscheidungsbefugt ist.

Anforderung / Umsetzung: Entscheidungskompetenz, Delegationsgrenzen und notwendige Fachfreigaben festlegen.

Erwarteter Nachweis: Mandat und F16 mit Bedingungen und Abweichungen.

Positivtest: Eine begründete Teilfreigabe mit passender Kompetenz treffen.

Negativ- oder Grenztest: Nicht akzeptiertes kritisches Risiko durch Projekttermin begründen lassen.

Abnahmekriterium: Zeit- oder Budgetdruck ersetzt keine erforderliche Fach- und Organentscheidung.

Aussagegrenze / Restrisiko: Formale Unterschriften garantieren keine informierte Entscheidung; Informationsqualität prüfen.

Grundlagen: [Q04; Q29]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K41 · Interdisziplinäre Entscheidung ohne Schattenorgan

Anwendung: Governance. **Verantwortung:** Leitung.

Problem: Ein neues Gremium hat keine Zuständigkeit oder überdeckt bestehende Fachverantwortung.

Anforderung / Umsetzung: Bestehendes oder neues Forum mit Mandat, Mitgliedern, Eskalation und Nachverfolgung einrichten, sofern Schnittstellen dies erfordern.

Erwarteter Nachweis: Geschäftsordnung und nachvollziehbare Beschlussakte.

Positivtest: Einen Konflikt zwischen Verfügbarkeit und Eingrenzung fachlich behandeln.

Negativ- oder Grenztest: Eine Entscheidung außerhalb des Gremienmandats vorlegen.

Abnahmekriterium: Zuständiger Entscheider und Fachbeteiligung bleiben klar; keine erfundene gesetzliche Pflicht zum benannten Board.

Aussagegrenze / Restrisiko: Sitzungszahl ist kein Wirksamkeitsnachweis.

Grundlagen: [Q04; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K42 · Beschaffung mit Abnahmebedingungen

Anwendung: Einkauf/Governance. **Verantwortung:** Einkauf mit Fachbetrieb/Security.

Problem: Werbeversprechen zu Sicherheit und Offlinefähigkeit werden ohne Test übernommen.

Anforderung / Umsetzung: Nicht zulässige Wirkung, Ausfallverhalten und erforderliche Nachweise schon in die Beschaffung aufnehmen.

Erwarteter Nachweis: F12, Leistungsbeschreibung und Abnahmeplan.

Positivtest: Eine kritische zugesagte Funktion unter genehmigten Bedingungen nachweisen.

Negativ- oder Grenztest: Widerspruch zwischen Offlineversprechen und zentraler Lizenzabhängigkeit prüfen.

Abnahmekriterium: Entscheidende Zusagen sind konkret nachweisbar oder als offene Beschaffungsbedingung geführt.

Aussagegrenze / Restrisiko: Lieferantenbelege gelten nur für ihren tatsächlichen Scope.

Grundlagen: [Q17; Q23]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K43 · Lieferantenänderung und Ausstieg

Anwendung: Einkauf/IT/OT. **Verantwortung:** Dienstleister-/Produkteigentümer.

Problem: Abhängigkeit von Herstellerzugang, Updates oder proprietärem Datenformat bleibt unbegrenzt.

Anforderung / Umsetzung: Support, Änderungen, Sicherheitsinformationen, Datenexport, Wiederherstellung und Vertragsende fachlich regeln.

Erwarteter Nachweis: Vertraglich geprüfte Anforderungen und Export-/Restoreprobe.

Positivtest: Einen begrenzten Daten-/Konfigurationsexport vollständig lesen und verwenden.

Negativ- oder Grenztest: Ausfall oder Supportende des Lieferanten im Szenario annehmen.

Abnahmekriterium: Wesentliche Betriebs- und Nachweisdaten bleiben im vereinbarten Umfang zugänglich; Grenzen sind bewusst entschieden.

Aussagegrenze / Restrisiko: Ein Export ist nicht automatisch in einem anderen Produkt verwendbar.

Grundlagen: [Q17; Q08]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K44 · Getrennte Meldespuren

Anwendung: Governance/Incident. **Verantwortung:** Benannte Meldestelle mit Recht/Datenschutz.

Problem: Eine Hersteller- oder Behördenmeldung wird fälschlich als Erfüllung aller Pflichten behandelt.

Anforderung / Umsetzung: Je Rechtsregime Auslöser, Kenntnis, Zuständigkeit, Frist, Empfänger und Nachmeldung führen.

Erwarteter Nachweis: F13 und geübte Kommunikationswege.

Positivtest: Einen synthetischen Mehrfachvorfall in getrennte Prüfspuren einordnen.

Negativ- oder Grenztest: Fehlende Detailkenntnis oder einen nicht meldepflichtigen Teilaspekt als Gegenfall prüfen.

Abnahmekriterium: Jede Entscheidung ist begründet und fristbezogen dokumentiert; offene Erkenntnisse erhalten Nachverfolgung.

Aussagegrenze / Restrisiko: Tatsächliche Meldepflicht und Fristbeginn hängen vom konkreten Fall ab.

Grundlagen: [Q29; Q37; Q38]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K45 · Datenschutz und Beschäftigtenrechte im Monitoring

Anwendung: Governance/Datenschutz. **Verantwortung:** Verantwortlicher mit Datenschutz- und Vertretungsbeteiligung.

Problem: Sicherheitsüberwachung wird ohne erforderliche Prüfung zur Personen- oder Leistungskontrolle erweitert.

Anforderung / Umsetzung: Zweck, Datenumfang, Zugriffe, Aufbewahrung und gegebenenfalls Mitbestimmung vor Einführung prüfen.

Erwarteter Nachweis: Verarbeitungskonzept und rechtlich geprüfte Beteiligung.

Positivtest: Sicherheitsfall mit minimal erforderlichen Daten nachvollziehen.

Negativ- oder Grenztest: Sicherheitslogs ohne festgelegten Zweck zur individuellen Leistungsbewertung nutzen wollen.

Abnahmekriterium: Unzulässige Zweckausweitung wird verhindert; Beteiligungs- und Rechtsprüfung ist dokumentiert.

Aussagegrenze / Restrisiko: Sektor-/Trägerbesonderheiten können andere Vertretungsregime erfordern.

Grundlagen: [Q32; Q38]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K46 · Befristete Ausnahmen

Anwendung: Governance. **Verantwortung:** Befugte Leitung mit Fachbewertung.

Problem: Vorläufige Vollrechte oder Ersatzkontrollen werden unbemerkt dauerhaft.

Anforderung / Umsetzung: Ausnahmen mit Risiko, Eigentümer, Ersatzkontrolle, Ende und Rücknahme dokumentieren.

Erwarteter Nachweis: F14 und Wiedervorlage.

Positivtest: Ausnahme im erlaubten Zeitraum mit Überwachung betreiben.

Negativ- oder Grenztest: Nutzung nach Ablauf oder außerhalb des genehmigten Scopes prüfen.

Abnahmekriterium: Keine automatische Verlängerung; kritische Funktion ohne weiter gültige Grundlage wird begrenzt.

Aussagegrenze / Restrisiko: Befristung allein reduziert die Gefahr nicht; Ersatzkontrolle muss wirken.

Grundlagen: [Q04; Q06]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K47 · Kompetenz und ausreichende Vertretung

Anwendung: Governance/Personal. **Verantwortung:** Leitung und Fachbereichsverantwortliche.

Problem: Neue Aufgaben sind formal verteilt, aber fachlich oder personell nicht leistbar.

Anforderung / Umsetzung: Benötigte Kompetenzen, Kapazität, Schulung und Vertretung aus Umfang und Betriebszeiten ableiten.

Erwarteter Nachweis: Qualifikations-/Vertretungsplan und beobachtete Übung.

Positivtest: Vertretung führt einen vorgesehenen kritischen Ablauf aus.

Negativ- oder Grenztest: Schlüsselperson, externer Dienst oder Hauptkommunikation fällt im Szenario aus.

Abnahmekriterium: Notwendige Handlungsfähigkeit ist nicht an eine unersetzte Einzelperson gebunden.

Aussagegrenze / Restrisiko: Keine pauschale Prognose neuer Stellenzahlen oder behaupteter neuer Berufsabschlüsse.

Grundlagen: [Q29; Q17]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K48 · Berichte mit Nachweisqualität statt Gesamtscore

Anwendung: Governance/Audit. **Verantwortung:** Risikomanagement und unabhängige Prüfung.

Problem: Hohe Dokumentationsquote verdeckt einen ungeklärten kritischen Schutzpfad.

Anforderung / Umsetzung: Scope, kritische Lücken, Ausnahmen und Evidenztiefe getrennt an Leitung berichten.

Erwarteter Nachweis: Leitungsbericht mit Kontroll- und Evidenzbezug.

Positivtest: Eine relevante Freigabe anhand des Berichts nachvollziehen.

Negativ- oder Grenztest: Viele positive Routinekontrollen gegen einen kritischen ungeklärten Befund aufrechnen.

Abnahmekriterium: Kritische Einzelbefunde bleiben sichtbar; Dokumentation wird nicht als Testnachweis gezählt.

Aussagegrenze / Restrisiko: Kennzahlen können bei veränderten Nennern scheinbar besser werden.

Grundlagen: [Q04; Q07]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K49 · Genehmigter Prüfumfang

Anwendung: Prüfung/Alle. **Verantwortung:** Prüfler mit Fachbetrieb.

Problem: Ein Sicherheitstest erzeugt selbst eine reale Versorgungs- oder Anlagenstörung.

Anforderung / Umsetzung: Testumgebung, Daten, Aktionen, Verantwortliche, Schutzmaßnahmen, Stopkriterien und Rückbau genehmigen.

Erwarteter Nachweis: F15 und separate Testfreigabe.

Positivtest: Zulässigen Test mit korrekter Beobachtung und Rückbau durchführen.

Negativ- oder Grenztest: Nicht genehmigte Liveaktion oder echte sensible Daten in die Prüfung aufnehmen wollen.

Abnahmekriterium: Grenzüberschreitung wird vor Wirkung gestoppt; Testgrenzen erscheinen im Bericht.

Aussagegrenze / Restrisiko: Simulation bildet reale Dynamik nicht vollständig ab; Übertragbarkeit gesondert bewerten.

Grundlagen: [Q02; Q05]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K50 · Positive und negative Testfälle

Anwendung: Prüfung. **Verantwortung:** Prüfverantwortliche.

Problem: Schutzwirkung wird nur an zulässigen Beispielen oder nur durch Blockieren aller Aktionen gezeigt.

Anforderung / Umsetzung: Für kritische Eigenschaften Referenz-, Gegen-, Fehler- und Umgehungsfälle mit vorherigem Sollverhalten planen.

Erwarteter Nachweis: P-Testfälle und reproduzierbare Beobachtungen.

Positivtest: Zulässige Leistung bleibt mit aktiver Kontrolle möglich.

Negativ- oder Grenztest: Unzulässige Aktion über einen alternativen oder veralteten Pfad prüfen.

Abnahmekriterium: Sowohl erforderliche Leistung als auch konkrete Grenze sind im Scope nachgewiesen.

Aussagegrenze / Restrisiko: Testabdeckung und angenommene Verteilung begrenzen statistische Schlussfolgerungen.

Grundlagen: [Q06; Q11]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K51 · Zeitmessung bis zur Wirkung

Anwendung: Prüfung/IAM/OT. **Verantwortung:** Prüfung mit IAM und Fachbetrieb.

Problem: Die gemeldete Sperrzeit endet am zentralen Server, nicht am kritischen Endpunkt.

Anforderung / Umsetzung: Erkennungs-, Entscheidungs-, Verteilungs- und Betriebsreaktionszeiten getrennt erfassen.

Erwarteter Nachweis: Zeitmessprotokoll mit synchronisierten beziehungsweise korrigierten Zeitquellen.

Positivtest: Definierten Widerruf bis zum relevanten Endverhalten verfolgen.

Negativ- oder Grenztest: Cache, Kommunikationsunterbrechung und laufenden Auftrag als Gegenfälle berücksichtigen.

Abnahmekriterium: Gemessene Wirkung und ihre Grenzen passen zu den lokal begründeten Zeitbedingungen.

Aussagegrenze / Restrisiko: Maximal beobachtete Zeit ist kein Beweis einer universellen oberen Schranke.

Grundlagen: [Q15; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K52 · Validierter Referenzzustand

Anwendung: Recovery. **Verantwortung:** Recovery-Leitung mit Facheigentümer.

Problem: Ein intaktes Backup oder eine Signatur wird als Beweis fachlich richtiger Daten ausgegeben.

Anforderung / Umsetzung: Herkunft, Zeitpunkt, technische Integrität, fachliche Prüfung und verbleibenden Verdacht getrennt dokumentieren.

Erwarteter Nachweis: Referenzakte und F10.

Positivtest: Einen ausgewählten Stand mit Herkunft und passenden Prüfungen begründen.

Negativ- oder Grenztest: Eine signierte, aber fachlich widersprüchliche Information in den Test aufnehmen.

Abnahmekriterium: Technische Echtheit wird nicht mit inhaltlicher Richtigkeit verwechselt; entscheidungsrelevante Unsicherheit bleibt begrenzt.

Aussagegrenze / Restrisiko: Keine absolute Aussage über Freiheit von unbekannter Manipulation.

Grundlagen: [Q08; Q22]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K53 · Getrennte und erprobte Wiederherstellungsressourcen

Anwendung: Recovery/IT/OT. **Verantwortung:** Backup-/Recovery-Verantwortung mit Betrieb.

Problem: Produktiver Zugriff zerstört zugleich Sicherung und benötigte Engineering-Unterlagen.

Anforderung / Umsetzung: Notwendige Daten, Programme, Konfigurationen, Dokumentation und Zugangsmittel geschützt und testbar vorhalten.

Erwarteter Nachweis: Wiederaufbauliste, Zugriffsmodell und Restoreprotokoll.

Positivtest: Benötigte Artefakte in einer kontrollierten Umgebung tatsächlich verwenden.

Negativ- oder Grenztest: Kompromittiertes Produktivadministratorkonto und Ausfall zentraler Ablage im Szenario annehmen.

Abnahmekriterium: Recovery hängt nicht ausschließlich von ungeschützten produktiven Kopien und Zugängen ab.

Aussagegrenze / Restrisiko: Backup kann fachlich falsche oder bereits kompromittierte Inhalte enthalten.

Grundlagen: [Q08; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K54 · Recovery-Bootstrap ohne Zirkelschluss

Anwendung: Recovery. **Verantwortung:** Recovery-Architektur.

Problem: Zum Wiederaufbau wird genau der ausgefallene Identitäts-, Lizenz- oder Managementdienst benötigt.

Anforderung / Umsetzung: Abhängigkeitszyklen identifizieren und vorbereiteten begrenzten Startpfad mit Notfalldokumentation testen.

Erwarteter Nachweis: Abhängigkeitsgraph und Bootstrap-Probe.

Positivtest: Minimalen Wiederaufbau mit genehmigten Notfallmitteln beginnen.

Negativ- oder Grenztest: Den regulären Verzeichnis-/Kommunikationsdienst als nicht verfügbar setzen.

Abnahmekriterium: Startpfad ist mit tatsächlich vorhandenen Ressourcen nutzbar und kontrolliert.

Aussagegrenze / Restrisiko: Notfallmittel dürfen nicht zu dauerhaften unkontrollierten Hintertüren werden.

Grundlagen: [Q08; Q07]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K55 · Nachvollziehbare Evidenzsicherung

Anwendung: Incident/Forensik. **Verantwortung:** Forensik-/Incident-Verantwortung.

Problem: Quellen werden verändert oder ohne Herkunft verteilt; spätere Aussagen sind nicht belastbar.

Anforderung / Umsetzung: Quelle, Erheber, Zeit, Methode, Integritätsmerkmal, Zugriff und Grenzen jedes relevanten Belegs erfassen.

Erwarteter Nachweis: Evidenzregister und geschützte Belegablage.

Positivtest: Gesicherten Beleg mit Quelle und unverändertem Zustand wiederfinden.

Negativ- oder Grenztest: Ein vom kompromittierten System erzeugtes Log als absolute Wahrheit behandeln wollen.

Abnahmekriterium: Herkunft und Aussagegrenze bleiben sichtbar; Schutz akuter Sicherheit hat Vorrang vor Vollständigkeit der Sicherung.

Aussagegrenze / Restrisiko: Unveränderte Ablage beweist nicht die Wahrheit des erzeugenden Systems.

Grundlagen: [Q05; Q38]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K56 · Eingrenzung mit Betriebsfolgen

Anwendung: Incident/Alle. **Verantwortung:** Incident Commander mit Fachbetrieb.

Problem: Eine technisch wirksame Maßnahme unterbricht unbemerkt eine kritische Leistung.

Anforderung / Umsetzung: Maßnahmenziel, betroffene Funktionen, Rücknahme, lokale Schutzwirkung und Fachfreigabe im Mandat abbilden.

Erwarteter Nachweis: F09 und entscheidungsbezogenes Ereignisprotokoll.

Positivtest: Begrenzte Maßnahme im sicheren Test mit bestätigter Wirkung durchführen.

Negativ- oder Grenztest: Gemeinsam genutzten Dienst als unerwartet betroffen vorgeben.

Abnahmekriterium: Folgen werden vor oder bei zeitkritischer Lage unmittelbar im genehmigten Verfahren fachlich beurteilt; kein blinder globaler Blackout.

Aussagegrenze / Restrisiko: Nicht jede Folge ist vorhersehbar; laufende Lagebewertung bleibt nötig.

Grundlagen: [Q05; Q02]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K57 · Getrennte Lage- und Meldekommunikation

Anwendung: Incident/Governance. **Verantwortung:** Kommunikations-/Meldestelle im Krisenmandat.

Problem: Technische Entwarnung wird als vollständige Versorgungserholung oder fehlender Datenabfluss verstanden.

Anforderung / Umsetzung: Bestätigte Fakten, Hypothesen, Einschränkungen, offene Abgleiche und Meldeentscheidungen getrennt kommunizieren.

Erwarteter Nachweis: Lageberichte mit Version und Verteiler; F13.

Positivtest: Adressatengerechte Meldung aus dem aktuellen Kenntnisstand erstellen.

Negativ- oder Grenztest: Formulierung kein Abfluss nachgewiesen in nachweislich kein Abfluss umdeuten.

Abnahmekriterium: Unsicherheit bleibt sprachlich korrekt; Empfänger und Folgeversion sind nachvollziehbar.

Aussagegrenze / Restrisiko: Kommunikation ersetzt weder technische Eingrenzung noch gesetzliche Einzelfallprüfung.

Grundlagen: [Q05; Q29; Q37]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K58 · Vollprozessübung mit Ressourcen

Anwendung: BCM/Prüfung. **Verantwortung:** BCM und Fachbetrieb.

Problem: Tabletop-Erfolg wird als Nachweis realer Ersatzbetriebsfähigkeit ausgegeben.

Anforderung / Umsetzung: Mindestens den freizugebenden kritischen Prozess mit Personal, Material, Kommunikation und Übergabe angemessen prüfen.

Erwarteter Nachweis: F08/F15 mit klarer Trennung simuliert/tatsächlich ausgeführt.

Positivtest: Synthetischen Fall vollständig im genehmigten Umfang bearbeiten.

Negativ- oder Grenztest: Ressourcenknappheit oder Schichtwechsel einspielen.

Abnahmekriterium: Erhaltbare Leistung und Erschöpfungsgrenze werden tatsächlich verstanden und dokumentiert.

Aussagegrenze / Restrisiko: Eine Übung belegt nur ihre Bedingungen; Wiederholung und angepasster Scope sind erforderlich.

Grundlagen: [Q18; Q07]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K59 · Abgleich realer und digitaler Ereignisse

Anwendung: Recovery/Fachbetrieb. **Verantwortung:** Fachliche Daten-/Qualitätsverantwortung.

Problem: Restore verwischt manuelle Vorgänge, Duplikate oder reale Zustandsänderungen.

Anforderung / Umsetzung: Ereignis- und Erfassungszeit, Quelle, Objektbezug, Konflikt und Entscheidung getrennt führen.

Erwarteter Nachweis: F11 mit Abgleichliste und offenen kritischen Punkten.

Positivtest: Synthetische Ersatzereignisse ohne Verlust ihrer Herkunft zusammenführen.

Negativ- oder Grenztest: Doppelauftrag, widersprüchlichen Stand oder spätere Erfassung prüfen.

Abnahmekriterium: Keine unkontrollierte Überschreibung; kritische Unklarheit verhindert die betroffene Folgeaktion.

Aussagegrenze / Restrisiko: Verbleibende Abgleicharbeit braucht Ressourcen und eine kontrollierte Frist.

Grundlagen: [Q18; Q08]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

K60 · Gestufte Wiederfreigabe und Nachprüfung

Anwendung: Recovery/Governance. **Verantwortung:** Befugte Betriebs-/Klinikleitung mit Fachprüfern.

Problem: Technischer Start wird als vollständige Betriebs-, Safety- und Datenfreigabe gewertet.

Anforderung / Umsetzung: Security, Technik, Fachbetrieb, erforderliche Schutzfunktionen und Daten-/Produktintegrität mit Bedingungen freigeben.

Erwarteter Nachweis: F10/F16; Nachprüftermine und eingeschränkte Agentenrechte.

Positivtest: Freigegebenen Teilumfang mit den zugehörigen Belegen aufnehmen.

Negativ- oder Grenztest: Offene kritische Integritäts- oder Schutzfrage trotz Projektzeitdruck zur Gesamtfreigabe stellen.

Abnahmekriterium: Nur nachgewiesener Umfang wird freigegeben; Bedingungen sind überwacht, Ausweitung benötigt eigenen Nachweis.

Aussagegrenze / Restrisiko: Eine erfolgreiche Wiederaufnahme beseitigt nicht die Notwendigkeit fortlaufender Überwachung und Ursachenarbeit.

Grundlagen: [Q05; Q02; Q04]. Eigene Ableitung; Zugriffstiefe und Fundstelle im Quellenregister beachten.

Lokale Bewertung: NICHT ERHOBEN. Nachweise E-... / Prüfungen P-... / Datum / Bearbeiter / Ergebnis / Entscheidung sind vom Anwender einzutragen.

Formularbuch · F01 bis F16

Ausfüllbare Arbeitsunterlagen für lokale Analyse, Prüfung und Freigabe

Verwendung: Diese Vorlagen werden für ein konkretes System kopiert, ausgefüllt und versioniert. Sie sind keine bereits erhobenen Betriebsnachweise. Angaben in eckigen Klammern sind auszufüllen. Synthetische Beispiele aus den Fallstudien dürfen nicht als reale Messwerte übernommen werden.

Dokumentenlenkung für jedes Formular: Kennung, System-/Leistungsbezug, Version, Datum, Ersteller, Prüfer, Freigabestelle, Vertraulichkeit und Ablageort. Ein Ablageort wie EVIDENZ/SYSTEM-01/ bezeichnet eine vorgeschlagene Organisationsstruktur; er behauptet keinen bereits vorhandenen Nutzerordner.

Vokabular: „Muss“ in einer lokalen Freigabe gilt nur, soweit die Organisation die Anforderung übernommen hat oder eine einschlägige Pflicht tatsächlich besteht. „Nicht anwendbar“ benötigt eine Begründung. „Offen“ darf nicht durch ein leeres Feld versteckt werden. Jede Unterschrift bezieht sich auf ihren fachlichen Umfang, nicht auf sämtliche möglichen rechtlichen und technischen Fragen.

F01 · System- und Leistungssteckbrief

Zweck: Die Einheit festlegen, für die eine Risiko- oder Freigabeaussage gelten soll. Ohne diesen Steckbrief sind spätere Prüfungen nicht eindeutig zuzuordnen. Zugehörige Kontrollen: K01, K02, K05.

Feld	Eintrag / Ausfüllregel
System-ID und Name	[eindeutige Kennung; kein bloßer Herstellername]
Fachliche Leistung	[Was wird für wen erbracht?]
Zulässiger Nutzen	[Erwarteter Nutzen ohne unbelegte Erfolgsquote]
Nicht zulässige Wirkung	[Konkrete Daten-, Freigabe- oder Steuerhandlungen]
Fachlicher / technischer Eigentümer	[Rollen und tatsächlich zuständige Personen]
KI-/Agentenfunktion	[lesen; Entwurf; schreiben; beauftragen; konfigurieren; bewegen]
Tatsächlich verwendete Versionen	[Modell, Tools, Integration, Betriebsstand]
Daten und betroffene Personen	[Kategorien und Zwecke; keine unnötigen Echtdaten]
Komponenten / Schnittstellen	[Verweise F02/F03]
Einsatzumgebung	[Standort, Betriebszeiten, Personalannahmen]
Erlaubte Betriebsmodi	[Verweise F08]
Nicht Teil dieser Freigabe	[ausgeschlossene Komponenten und Funktionen]
Rechtliche Scopeprüfung	[Verweis F06; offene Fragen sichtbar]
Nächster Wiederprüfauslöser	[Änderung, Vorfall, Frist oder neue Verbindung]

Auswertung: Der Leser muss erkennen können, welche Aussage nach diesem Steckbrief gerade nicht zulässig wäre. „KI sicher“ ist zu weit; „Agent A darf im Stand V Entwürfe für Prozess P ohne Freigaberecht erstellen“ ist prüfbar. Ein Vollständigkeitsproblem bleibt offen, wenn notwendige Teilprozesse außerhalb der Grenze liegen und niemand für deren Schnittstelle verantwortlich ist.

Typischer Fehler: Der Scope beschreibt die Software, während das anschließende Audit einen klinischen oder industriellen Gesamtnutzen behauptet. Dies ist vor der Prüfung zu korrigieren.

F02 · Abhängigkeits- und Datenflussregister

Zweck: Verbindungen und notwendige Voraussetzungen der Leistung erfassen. Pro Fluss beziehungsweise Abhängigkeit wird ein Datensatz angelegt. Zugehörige Kontrollen: K02, K03, K14, K21, K54.

Feld	Eintrag / Ausfüllregel
Fluss-/Abhängigkeits-ID	[D-...]
Quell- und Zielkomponente	[eindeutige Systemkennungen]
Fachlicher Zweck	[Warum ist diese Verbindung erforderlich?]
Datenobjekte / Operation	[nicht nur Port oder Protokoll]
Vertrauensgrenze	[intern/extern; Betreiber; zuständige Identitätsinstanz]
Benötigte Grundlage	[Zeit, DNS, Identity, Strom, Lizenz, Herstellerdienst]
Ausfall- und Integritätsfolge	[nicht verfügbar / falsch / veraltet / fehlzugeordnet]

Feld	Eintrag / Ausfüllregel
Erhaltene Alternative	[konkret; nicht pauschal „manuell“]
Gemeinsame Ursache	[weitere betroffene Leistungen oder Schutzfunktionen]
Konfigurations-/Beobachtungsbeleg	[E-... mit Datum und Zugriffstiefe]
Eigentümer	[Verantwortlicher für diesen Pfad]
Offene Frage	[Fehlende Herstellerinformation oder ungeprüfter Pfad]

Prüfung: Einen real vorgesehenen, aber synthetisch ausgeführten Geschäftsvorgang durch das Register verfolgen. Seltene Fernwartungs-, Update- und Notfallpfade gesondert prüfen. Bei OT keine ungeprüften aktiven Scans zur vermeintlich schnellen Vollständigkeit verwenden.

Ergebnisregel: Ein unbekannter Pfad wird nicht automatisch gelöscht. Zunächst wird sein Zweck geklärt. Ist seine kritische Wirkung nicht begrenzt, verhindert das die Freigabe dieses Pfads, bis eine geeignete Entscheidung vorliegt.

F03 · Register der Handlungsvollmachten

Zweck: Verbindung ist nicht Autorisierung. Dieses Formular beschreibt, wer eine konkrete Handlung ausführen darf. Zugehörige Kontrollen: K22, K29–K36.

Feld	Eintrag / Ausfüllregel
Mandats-ID	[A-...; eindeutiger Widerrufsbezug]
Ausführende Identität	[Mensch, Dienst, Agent, Subagent, Gerät]
Verantwortlicher Auftraggeber	[Organisation und Rolle]
Ressource / Objektbereich	[genaue Daten- oder Systemgrenze]
Erlaubte Aktionen	[explizite Liste]
Verbotene / nicht vergebene Aktionen	[kritische Gegenfälle]
Zweck / Auftrag	[begründeter Bezug]
Kontextquelle	[wer bestätigt Auftrag, Betriebsmodus und Version?]
Beginn / Ende	[Zeitzone und gültige Zeitbedingungen]
Unterdelegation	[zulässig? Umfang, Tiefe, Dauer]
Zusätzlich erforderliche Freigabe	[Fachrolle, Schwelle und Nachweis]
Widerrufsmechanismus	[nicht nur Kontosperrung; Endpunktwirkung]
Restverhalten	[Sessions, Queue, laufender Prozess]
Nachweise	[Policy E-...; Tests P-...]

Synthetisches Beispiel: Ein Planungsagent liest die freigegebene Auftragsliste eines Testbereichs und erzeugt Entwürfe. Er besitzt keine Freigabe- oder Maschinenparameterrechte. Eine Unterdelegation darf nur ausgewählte Leseobjekte umfassen. Dieses Beispiel wird in BEISPIEL_AUTHORITY_REGISTER.json maschinenlesbar mitgeführt.

Abnahmekriterium: Ein nicht vorgesehener Aufruf muss am tatsächlichen Ziel wirkungslos bleiben; die notwendige erlaubte Aktion muss weiterhin möglich sein. Das Formular allein ist keine technische Durchsetzung.

F04 · Risiko- und Gefährdungsfall

Zweck: Ein konkreter unerwünschter Verlust wird mit seinem Entstehungspfad verbunden. Zugehörige Kontrollen: K04, K20, K23, K26.

Feld	Eintrag / Ausfüllregel
Szenario-ID	[R-...]
Möglicher Verlust	[Person, Versorgung, Produkt, Umwelt, Daten, Betrieb]
Gefährlicher / unzulässiger Zustand	[Was wäre unmittelbar problematisch?]

Feld	Eintrag / Ausfüllregel
Auslösender Akteur oder Fehler	[Zugriff und Fähigkeiten; alternativ nicht böswilliger Fehler]
Eintritts-/Voraussetzungsbedingungen	[keine unbelegte pauschale Wahrscheinlichkeit]
Wirkungskette	[Schrittfolge mit System-/Datenbezug]
Betroffene Betriebsmodi	[Normal-, Ersatz- und Wiederanlauf]
Zeit bis möglicher Wirkung	[fachlich hergeleitet oder ausdrücklich unbekannt]
Umkehrbarkeit	[reversibel; nur begrenzt; irreversibel; unklar]
Barrieren	[Kontrollkennungen und Nachweisstatus]
Gemeinsame Ursachen / Umgehungen	[Kann ein Zugriff mehrere Barrieren verändern?]
Restrisiko und Unsicherheit	[offene Annahmen und Beweisgrenzen]
Entscheidung	[begrenzen, prüfen, vermeiden, unter Bedingungen akzeptieren]

Bewertung: Auswirkungen bleiben mehrdimensional. Eine geringe wirtschaftliche Wirkung darf eine relevante Personengefährdung nicht rechnerisch neutralisieren. Wo ordinal klassifiziert wird, werden Klassen definiert und nicht ohne Begründung multipliziert.

Gegenprobe: Die Kette zusätzlich mit einer fehlerhaften legitimen Handlung statt eines Angreifers durchdenken. Dadurch werden Schutzmaßnahmen sichtbar, die auch gegen Konfigurationsfehler und autonome Fehlentscheidungen wirken müssen.

F05 · Begründeter Nachweisfall

Zweck: Eine Freigabebehauptung so strukturieren, dass ein Dritter sie nachvollziehen und angreifen kann. Zugehörige Kontrollen: K06, K48, K50, K60.

Feld	Eintrag / Ausfüllregel
Behauptungs-ID	[N-...]
Präzise Behauptung	[System, Eigenschaft, Stand, Umfang]
Risiko-/Pflichtenbezug	[R-...; passende Q-Fundstelle]
Argument	[Warum tragen die Nachweise diese Behauptung?]
Positive Evidenz	[E-... mit tatsächlicher Zugriffstiefe]
Gegenbelege / Gegenproben	[P-... und widersprechende Beobachtung]
Annahmen	[Vertrauensanker, Umgebung, Personal, Version]
Nicht nachgewiesen	[sichtbare Begrenzung]
Fachbewertung	[zuständige Rolle und Begründung]
Freigabefolge	[voll für diesen Scope; eingeschränkt; gesperrt]
Ablauf / Wiederprüfung	[konkreter Auslöser]

Beispielhafte Argumentform: „Die Schnittstelle nimmt ausschließlich die in E-12 dokumentierten Entwurfsoperationen an. P-04 zeigt den zulässigen Vorgang, P-05 die Ablehnung einer Freigabeänderung. Nicht geprüft ist das Altsystem Z; es ist nicht in der Freigabe enthalten.“ Die Kennungen sind Muster, keine tatsächlich vorhandenen Anwendernachweise.

Fehlervermeidung: Der Satz „Alle Tests grün“ ist kein Argument, solange weder Testpopulation noch Gegenfälle und Systemstand erkennbar sind.

F06 · Rollen, Rechtsanwendbarkeit und Zuständigkeiten

Zweck: Mehrere Pflichtenregime und Entscheidungsrollen sauber trennen. Zugehörige Kontrollen: K05, K07, K39–K41, K45.

Feld	Eintrag / Ausfüllregel
Organisation / Träger	[Rechtsträger; keine reine Produktmarke]
Vorgang / System	[F01-Bezug]
Mögliche Rechtsrolle	[Betreiber, Arbeitgeber, Hersteller, KI-Anbieter/-Betreiber, Datenverantwortlicher usw.]
Anwendungsfakten	[Leistung, Größe, Produkt, Verwendungszweck, Datenbezug]
Rechtsgrundlage	[aktueller Text, Paragraph/Artikel, Status]
Einstufung	[anwendbar; nicht anwendbar mit Begründung; offen]
Zuständige Fachprüfung	[Recht, Klinik, Safety, Datenschutz usw.]
Entscheidungsbefugnis	[wer entscheidet diesen konkreten Punkt?]
Ausführung / Mitwirkung / Information	[rollenbezogen]
Vertretung	[benannt und nutzbar]
Offener Volltext-/Normencheck	[keine leeren Statusfelder]
Wiederprüfauslöser	[Änderung, Wachstum, neue Nutzung, Rechtsänderung]

Hinweis: Die Quelle Q38 ist im externen Register nicht als aktuell vollständig gelesener Normtext markiert. Für die lokale Rechtsakte muss daher der tatsächlich verwendete Volltext ergänzend dokumentiert werden. Dasselbe Prinzip gilt für Q39–Q41 und lizenzierte Normen.

Ergebnisregel: Eine offene entscheidende Einstufung erlaubt keine uneingeschränkte Behauptung vollständiger Rechtskonformität. Technische Schutzmaßnahmen können dennoch sachgerecht vorbereitet und umgesetzt werden.

F07 · Änderungs- und Rollbackentscheidung

Zweck: Wirkung, Rechte und Nachweise bei Änderungen gemeinsam prüfen. Zugehörige Kontrollen: K19, K24, K30, K43.

Feld	Eintrag / Ausfüllregel
Change-ID und Anlass	[C-...]
Alter / neuer Stand	[Modell, Tools, Schema, Parameter, Rechte, Datenquellen]
Geänderte Wirkung	[Welche neue oder andere Handlung wird möglich?]
Betroffene Risiken / Nachweise	[R-...; N-...; K-...]
Benötigte Tests	[Referenz-, Gegen-, Fehler- und Regressionstest]
Fachliche / rechtliche Mitprüfung	[einschlägiger Scope]
Wartungs-/Einführungsbedingungen	[Personal, Betriebsmodus, Kommunikation]
Rollback-Artefakte	[tatsächlich verfügbar und kompatibel]
Daten-/Schemafolgen	[Kann ein Rückschritt neue Daten noch lesen?]
Abbruchbedingung	[vor Umsetzung festgelegt]
Freigabe	[befugte Rolle, Bedingungen, Datum]
Nachbeobachtung	[Messpunkte und Endentscheidung]

Prüfung: Ein Update ohne neue Modellnummer kann trotzdem neue Rechte oder Datenflüsse erzeugen. Umgekehrt muss ein rein redaktioneller Textwechsel nicht dieselben Prüfungen auslösen wie eine neue Steuerfunktion. Die Bewertung folgt dem veränderten Wirkungspfad.

Ergebnisregel: Fehlender Rollback wird nicht durch eine deklarierte „Rücksetzoption“ ersetzt. Wenn Rückbau technisch nicht möglich ist, muss die Freigabe diese Irreversibilität ausdrücklich berücksichtigen.

F08 · Betriebsmodus und sichere Mindestleistung

Zweck: Ersatzbetrieb als zeitlich und fachlich begrenzte Leistung beschreiben. Zugehörige Kontrollen: K08, K15–K17, K25–K26, K58.

Feld	Eintrag / Ausfüllregel
Modus-ID	[M-...; nicht zwingend linear]
Auslöser / Eintrittskriterium	[beobachtbarer Zustand]
Erhaltene Leistung	[konkret und fachlich bestätigt]
Verlorene / eingeschränkte Funktion	[einschließlich Alarmierung und Dokumentation]
Benötigte Daten und Technik	[lokale Grundlagen und Vertrauensstatus]
Benötigtes Personal / Material	[Qualifikation, Anzahl lokal bestimmen, Verfügbarkeit]
Maximal vertretbare Dauer	[fachlich hergeleitet; keine universelle Vorgabe]
Kontrollpunkte	[wie wird Tragfähigkeit beobachtet?]
Entscheidungs- und Ausführungsrolle	[mit Vertretung]
Eskalation bei Erschöpfung	[nächste geeignete Einschränkung / externe Abstimmung]
Rückkehrbedingung	[welche Nachweise sind erforderlich?]
Geübter Umfang / Grenze	[was wurde wirklich durchgeführt?]

Interpretation: „Lokal verfügbar“ bedeutet nicht automatisch „Versorgung unverändert“. Personelle Präsenz, Kommunikation und Arbeitsabläufe können sich ändern. Bei Maschinen können Restenergie und Prozessmedien auch im Stillstand erforderlich bleiben.

Abnahme: Eine Tabletop-Diskussion kann das Verfahren verbessern, ersetzt aber nicht den technischen oder fachlichen Nachweis der tatsächlich behaupteten Ersatzleistung.

F09 · Mandat für Cyber-Eingrenzung und defensive Agenten

Zweck: Gegenmaßnahmen so begrenzen, dass ein Fehlalarm keine unkontrollierte Betriebswirkung erzeugt. Zugehörige Kontrollen: K35, K37, K38, K56.

Feld	Eintrag / Ausfüllregel
Mandats-ID / ausführender Akteur	[SOC, Automatisierung, Agent, lokale Fachrolle]
Auslösende Beobachtung	[Signal und erforderliche Bestätigung]
Erlaubte Aktion	[genaues Ziel und Umfang]
Nicht erlaubte Aktion	[kritische Gegenfälle]
Maximaler Wirkungsumfang	[Systeme, Daten, Laufzeit; lokal begründet]
Erwartete Betriebsfolge	[einschließlich Nebenwirkung]
Benötigte Fachfreigabe	[vorab / ereignisbezogen / lokale Schutzlogik]
Verhalten bei Unsicherheit	[nicht pauschal alles erlauben oder abschalten]
Rücknahme und Restwirkung	[Queue, Session, physischer Prozess]
Wirkungsbestätigung	[unabhängige oder ausreichend geeignete Beobachtung]
Protokollierung	[Ereignis, Entscheidung, Ausführung, Ergebnis]
Nachprüfung	[wer kontrolliert den Eingriff?]

Beispiel: Die Sperre neuer externer Exportaufträge kann für einen eng begrenzten Dienst vorab erlaubt sein. Daraus folgt keine Vollmacht zur Abschaltung einer gemeinsamen Identitäts- oder Alarmierungsplattform. Ob der Exportblock selbst Versorgung beeinträchtigt, ist vorher zu prüfen.

Sperrregel: Eine Maßnahme ohne verstandene kritische Betriebsfolge ist nicht allein wegen eines hohen Detektionsscores automatisch freigegeben.

F10 · Wiederaufbau und gestufte Wiederfreigabe

Zweck: Technischen Start mit fachlicher Betriebsfähigkeit verbinden. Zugehörige Kontrollen: K28, K52–K54, K60.

Feld	Eintrag / Ausfüllregel
Recovery-ID / Leistung	[W-...]
Gewählter Referenzstand	[Datum, Version, Herkunft]
Vertrauensbegründung	[technische und fachliche Prüfung getrennt]
Bekannte Unsicherheit	[Kontamination, Lücken, ungeprüfte Daten]
Notwendige Artefakte	[Daten, Programme, Konfiguration, Dokumentation]
Startpfad und Abhängigkeitszyklen	[Identity, Zeit, Netzwerk, Speicher, Lizenz]
Geänderte Geheimnisse / Rechte	[nach Verdachtsumfang]
Wiederaufbauschritte	[anlagen-/leistungsspezifisch]
Technischer Nachweis	[E-/P-Kennungen]
Fach-/Safety-/Qualitätsnachweis	[zuständige Rolle und Scope]
Offener Ereignisabgleich	[F11]
Freigegebene Teilfunktionen	[Agentenrechte ausdrücklich nennen]
Bedingungen und Rücknahme	[konkrete Grenzen]

Abnahme: „Backup eingespielt“ ist ein Teilergebnis. Die Freigabe verlangt den zur Leistung passenden Nachweis. Ein Hash unterstützt Integritätsprüfung, bestätigt aber nicht die medizinische oder prozesstechnische Richtigkeit eines Inhalts.

F11 · Ereignisabgleich und Konfliktentscheidung

Zweck: Reale Vorgänge aus dem Ersatzbetrieb mit der wiederhergestellten digitalen Umgebung nachvollziehbar zusammenführen. Zugehörige Kontrollen: K18, K28, K59.

Feld	Eintrag / Ausfüllregel
Ereignis-ID	[X-...; im Ersatzprozess eindeutig]
Reales Ereignisdatum / -zeit	[einschließlich Unsicherheit und Zeitzone]
Spätere Erfassungszeit	[separat, nicht als Ereigniszeit ausgeben]
Quelle / Urheber	[Papier, Gerät, Person, anderes System]
Personen-/Auftrags-/Produktbezug	[geeignete Kennung; keine unnötigen Kopien]
Inhalt / Art der Änderung	[fachlich notwendiger Umfang]
Bereits digital vorhandener Bezug	[bestehender Datensatz / Konflikt]
Konflikttyp	[Dublette, Widerspruch, fehlender Bezug, Versionsproblem]
Bedeutung für weitere Handlungen	[kritisch, begrenzt, ungeklärt; lokal definieren]
Fachentscheidung	[Bestätigung, Korrektur, weitere Prüfung; kein stilles Überschreiben]
Ausführender / Freigebender	[mit Zeit]
Abschluss / verbleibende Bedingung	[offene Punkte sichtbar]

Beispiel: Ein im Ersatzbetrieb erledigter synthetischer Auftrag darf nach Restore nicht erneut ausgelöst werden. Der Abgleich verknüpft seine tatsächliche Erledigung mit dem digitalen offenen Auftrag und bewahrt die Herkunft der Information.

Grenze: Vollständigkeit hängt von der Qualität der Ersatzdokumentation ab. Unklare Angaben werden nicht durch einen automatisierten Import „geheilt“.

F12 · Lieferanten-, Produkt- und Vertragsnachweise

Zweck: Aus einer Sicherheitszusage eine prüfbare Beschaffungsanforderung machen. Zugehörige Kontrollen: K15, K22, K42, K43.

Anforderungsthema	Nachweis und offene Frage
Zweckbestimmung und Systemgrenze	[Welche Verwendung und welche ausdrücklich nicht?]
Lokaler / eingeschränkter Betrieb	[Welche Funktionen bleiben ohne externe Dienste?]
Identitäten und Rechte	[Mandat, Fernwartung, Unterdelegation, Widerruf]
Sicherheitsupdates / Supportende	[Dauer, Verantwortlicher, Ablauf, Kompatibilität]
Schwachstellen- und Incident-Meldung	[Kontakt, Informationsumfang, Unterstützung]
Konfiguration und Änderungsinformation	[Versionierung und Benachrichtigung]
Protokollierung	[Felder, Zugriff, Export, Integrität, Datenschutz]
Daten und Unterauftragnehmer	[Empfänger, Zwecke, Speicher, Rückgabe/Löschung]
Backup und Wiederherstellung	[benötigte Artefakte und geprüfter Ablauf]
Ausstieg / Migration	[Nutzbarkeit der exportierten Daten und Konfiguration]
Nachweise Dritter	[Scope, Version, Datum, Prüfstelle]
Geplante Abnahme	[Test und Sollverhalten]

Bewertungsregel: „Ja“ ist keine ausreichende Antwort, wenn eine kritische Eigenschaft nachgewiesen werden muss. Pro Position werden Beleg, Scope, offene Abweichung und Entscheidung geführt. Ein Zertifikat wird nur für den tatsächlich geprüften Gegenstand anerkannt.

Vertragsgrenze: Dieses Formular ist kein Vertragsmuster. Die Übernahme in Ausschreibung oder Vertrag erfordert eine passende rechtliche und gegebenenfalls vergaberechtliche Prüfung.

F13 · Incident- und Meldeentscheidungen

Zweck: Mehrere gesetzliche und vertragliche Prüfspuren unabhängig und fristbezogen führen. Zugehörige Kontrollen: K44, K55, K57.

Feld	Eintrag / Ausfüllregel
Vorfall-ID	[I-...]
Beobachtung / Kenntnisstand	[Fakten getrennt von Hypothesen]
Kenntniszeitpunkt je möglichem Tatbestand	[nicht automatisch gleich erster Alarm]
Betroffene Leistung / Daten / Produkt	[Scopes getrennt]
Mögliche Pflicht	[BSIG; Datenschutz; CRA; weitere einschlägige Regel]
Anwendungs- und Risikoprüfung	[Bearbeiter, Begründung, offene Frage]
Meldeentscheidung	[ja; nein mit Begründung; laufende Prüfung]
Früheste Handlung / späteste Frist	[unverzüglich nicht als Warten bis Fristende interpretieren]
Zuständiger Empfänger / Weg	[aktueller behördlicher oder vertraglicher Kanal]
Gesendete Fassung / Zeit / Empfang	[nachweisbar]
Ergänzung / nächste Prüfung	[konkret]
Information Betroffener / Öffentlichkeit	[gesonderte Entscheidung und Grundlage]

Wichtig: Eine 72-Stunden-Zahl macht zwei Rechtsverfahren nicht identisch. Auslöser, Empfänger, Risikomaßstab und Abschlussbericht unterscheiden sich. Q29 § 32 und Q37 sind am Stichtag gelesen; Q38 verweist zusätzlich auf den erforderlichen lokalen DSGVO-Volltextcheck.

Beispielrechnung, keine Einstufung: Wird in einem einschlägigen Beispiel am 25.09.2026 um 10:00 Uhr MESZ der maßgebliche Kenntnisstand erreicht, lägen rechnerisch 24 Stunden später der 26.09. um 10:00 Uhr und 72 Stunden später der 28.09. um 10:00 Uhr. Ob genau diese Uhr startet, muss juristisch/fachlich festgestellt werden; die Pflicht

zur unverzüglichen Handlung bleibt getrennt.

F14 · Befristete Ausnahme und Restrisiko

Zweck: Eine Abweichung bewusst und nachprüfbar behandeln, statt sie als Dauerprovisorium verschwinden zu lassen. Zugehörige Kontrollen: K27, K40, K46.

Feld	Eintrag / Ausfüllregel
Ausnahme-ID und betroffene Kontrolle	[EX-...; K-...]
Abweichung	[tatsächliche fehlende Eigenschaft]
Grund und geprüfte Alternativen	[warum derzeit nicht anders?]
Mögliche Wirkung / Restrisiko	[R-... mit Unsicherheit]
Kompensierende Maßnahme	[konkret und geprüft]
Zulässiger Umfang	[welche Nutzung bleibt erlaubt?]
Nicht erlaubte Nutzung	[kritische Grenze]
Entscheidungskompetenz	[Mandat und Fachbeteiligung]
Beginn / Ende	[keine automatische Verlängerung]
Überwachung und Rücknahme	[wer prüft was?]
Ablöse-/Korrekturplan	[Verantwortlicher, Ressourcen, Nachweisziel]

Bewertung: Eine Ausnahme ist nur tragfähig, wenn ihr Risiko verstanden und ihre Ersatzkontrolle wirksam ist. Eine fehlende letzte Schutzfunktion kann nicht durch die bloße Unterschrift eines fachlich unzuständigen Projektleiters kompensiert werden.

Ergebnisregel: Bei Ablauf ist neu zu entscheiden oder die betroffene zusätzliche Nutzung zu beenden. Eine automatische Verlängerung wäre eine nicht begründete neue Risikoakzeptanz.

F15 · Prüf- und Übungsprotokoll

Zweck: Beobachtung und Sollverhalten nachvollziehbar verbinden. Zugehörige Kontrollen: K49–K51, K58.

Feld	Eintrag / Ausfüllregel
Prüf-ID und Ziel	[P-...; K-/N-Bezug]
Prüfumgebung und Stand	[isoliert, Simulation, Testsystem, gesondert genehmigter Betrieb]
Tatsächlich / nur simuliert	[klar getrennt]
Daten und Berechtigungen	[synthetisch / zulässiger Scope]
Vorausgesetzter Zustand	[Version, Konfiguration, Personal, Netz]
Eingabe / Ereignis	[reproduzierbar ohne gefährliche Liveanleitung]
Erwartetes Verhalten	[vor Durchführung festgelegt]
Tatsächliche Beobachtung	[Messung; nicht nachträgliche Behauptung des Agenten allein]
Messpunkte und Zeitbasis	[Quelle, Korrektur, Unsicherheit]
Positiv- / Negativfall	[beide zuordnen]
Stopkriterium / Rückbau	[genehmigt]
Ergebnis und Gegenbefund	[erfüllt; teilweise; nicht erfüllt; nicht ausgeführt]
Einschränkung der Aussage	[was folgt nicht aus dem Test?]
Korrektur / Wiederholung	[Verantwortlicher und Nachweis]

Statistische Grenze: Die Anzahl bestandener Tests ist ohne Auswahlmodell und Abdeckung kein Maß einer realen Angriffsquote. Band 6 erläutert die mathematischen und praktischen Grenzen.

F16 · Ausschussentscheidung und Betriebsfreigabe

Zweck: Den tatsächlich nachgewiesenen Nutzungsumfang verbindlich entscheiden. Zugehörige Kontrollen: K40, K48, K60.

Feld	Eintrag / Ausfüllregel
Entscheidungs-ID / Anlass	[B-...]
Freizugebender Scope	[F01; Version; Funktion]
Entscheidungsgrundlagen	[N-/E-/P-Kennungen und Rechtsprüfung]
Wesentliche positive Nachweise	[keine reine Prozentangabe]
Kritische Gegenbefunde	[auch abweichende Fachmeinungen]
Offene Punkte	[Risiko, Verantwortlicher, Wirkung auf Freigabe]
Entscheidung	[freigegeben; begrenzt; nicht freigegeben]
Bedingungen	[Nutzungsgrenze, Überwachung, Ablauf]
Nicht freigegebene Funktion	[ausdrücklich benennen]
Befugte Entscheidung und Fachmitfreigaben	[jeweils mit eigenem Umfang]
Kommunikation	[wer muss die Bedingungen kennen?]
Wiederprüfung / Rücknahmeauslöser	[konkret und beobachtbar]

Schlussformel: „Freigegeben ist ausschließlich [Umfang] im Stand [Version] unter [Bedingungen]. Die Freigabe stützt sich auf [Nachweise]. Nicht nachgewiesen beziehungsweise ausgeschlossen sind [Punkte]. Bei [Auslöser] ist die Nutzung einzuschränken und erneut zu bewerten.“

Eine solche Entscheidung ist stärker als ein uneingeschränktes Gütesiegel, weil sie Gegenstand, Evidenz und Grenzen offenlegt. Sie ersetzt keine notwendige gesetzliche Konformitätsbewertung oder behördliche Entscheidung.

Drei durchgängige Fallstudien

Von einer plausiblen Störung zur begründeten Betriebsentscheidung

Verwendung: Die Beispiele verbinden die sechs Fachbände, den Kontrollkatalog und das Formularbuch. Sämtliche Organisationen, Systemzusammenstellungen, Zeitfolgen und angenommenen Befunde sind erfunden. Die Beispiele belegen keine Häufigkeit und keine tatsächliche Leistungsfähigkeit einer Klinik, Fabrik oder Abwehrlösung. Die jeweils beschriebenen Prüfergebnisse sind **Erwartungen an einen künftigen Test**, keine erhobenen Ergebnisse.

Die Fälle sind absichtlich nicht auf den spektakulärsten Angriff zugeschnitten. Sie behandeln schwierige Zwischenzustände: eine Klinik mit zweifelhaften, aber weiter verfügbaren Informationen; eine Fabrik mit wirksamer lokaler Safety, aber gefährdeter Produktintegrität; und eine Abwehr, deren überbreite Reaktion selbst zum Ausfall führen könnte. Die technische und organisatorische Grundlage liefern Q02, Q05, Q07, Q13–Q17 und Q22. Die konkrete Zusammenstellung ist eine eigene analytische Synthese.

S-KLINIK · Die Systeme laufen, aber ein Befund ist nicht mehr eindeutig zuzuordnen

1. Auftrag, Systemgrenze und Annahmen

Eine fiktive Klinik verwendet ein Krankenhausinformationssystem, ein Laborinformationssystem, eine Integrationsplattform und einen KI-Dienst, der für ärztliche Nutzer Zusammenfassungen vorbereitet. Der Dienst darf ausgewählte Informationen lesen und Entwürfe in einen getrennten Arbeitsbereich schreiben. Er darf weder Stammdaten ändern noch Befunde freigeben oder eine Therapieanordnung auslösen. Die ärztliche Bewertung bleibt ein eigener Arbeitsprozess. Eine solche Rollenbegrenzung ist eine Entwurfsannahme des Beispiels, keine Behauptung über alle verfügbaren klinischen KI-Produkte. [Q16, Security; Q17, CPGs; Q22, Risikomanagement über den Lebenszyklus]

Die Prüfung umfasst den Weg von der Patientenidentifikation über Auftrag, Probe, Ergebnis, Integration und Zusammenfassung bis zur fachlichen Kenntnisaufnahme. Eine Untersuchung nur der KI-Schnittstelle wäre zu eng. Nicht untersucht werden die analytische Genauigkeit des Laborverfahrens und individuelle Therapieentscheidungen; dafür sind andere Fachprüfungen erforderlich.

Als Störung wird angenommen, dass eine Nachricht formal gültig ist, aber eine widersprüchliche Zuordnung zwischen Patientenidentifikation und Auftragsidentifikation enthält. Noch ist unklar, ob ein Bedienfehler, ein Schnittstellenfehler oder ein absichtlicher Eingriff vorliegt. Gerade diese Unklarheit begründet den Fall. Für den Schutz der Versorgung muss die Ursache nicht bereits abschließend als Cyberangriff attribuiert sein.

2. Schadenshypothese und Gegenhypothesen

Die primäre Wirkungskette lautet: widersprüchliche Zuordnung → unbemerkte Übernahme in eine Zusammenfassung → fachlich nicht zum Patienten passende Information erscheint glaubwürdig → eine Entscheidung wird auf falscher Grundlage getroffen. Die mögliche Folge ist klinisch relevant, wird hier aber weder als eingetretener Schaden noch durch ein konkretes Behandlungsszenario behauptet.

Gegenhypothesen sind ausdrücklich zu prüfen: Vielleicht ist nur die Darstellung falsch, während die freigegebene Primärinformation korrekt zugeordnet ist. Vielleicht gehört der Befund zu einem gültigen, zusammengeführten Fall, dessen Historie die Oberfläche nicht zeigt. Vielleicht liegen mehrere Patientenidentitäten tatsächlich irrtümlich zusammen. Eine globale Datenrücksetzung ohne diese Unterscheidung könnte richtige neue Informationen beseitigen. Ein bloßes „Die KI halluziniert“ würde umgekehrt eine fehlerhafte Quellintegration übersehen.

Die zu schützende Größe ist daher zunächst die **belegte Zuordnung und Verwendbarkeit konkreter Informationen**. Der allgemeine Betriebsstatus der Anwendung ist kein hinreichender Ersatzindikator. Für die Prüfung werden F01, F02 und F04 eröffnet; das Risiko erhält im Beispiel die Kennung R-K01.

3. Erstentscheidung und begrenzte Eingrenzung

Der Vorfall wird an die klinische Entscheidungsfunktion und die technische Einsatzleitung gemeinsam eskaliert. Der betroffene Zusammenfassungspfad kann in einen Modus ohne neue patientenbezogene Ausgaben überführt werden, sofern der festgelegte klinische Ersatzprozess verfügbar ist. Die Entscheidung bezieht sich auf einen identifizierten Pfad; sie setzt nicht automatisch das gesamte Krankenhausinformationssystem außer Betrieb.

Gleichzeitig sind betroffene Entwürfe gegen ungeprüfte Weiterverwendung zu kennzeichnen und technische Evidenz zu sichern. Bereits fachlich verwendete Ausgaben werden nicht still überschrieben. Sie benötigen eine nachvollziehbare fachliche Bewertung und gegebenenfalls einen dokumentierten Korrekturprozess. Ob weitere klinische Maßnahmen erforderlich sind, entscheidet die zuständige klinische Stelle anhand der realen Befunde. Dieser Leitfaden gibt dazu keine Therapieanweisung.

Die Zugriffsbeschränkung auf den KI-Dienst allein wäre unzureichend, wenn die fehlerhafte Zuordnung auch direkt in die klinische Hauptanwendung gelangt. Dann erweitert sich der Scope der Eingrenzung. Genau deshalb müssen F02 und das tatsächliche Nachrichtenrouting zugänglich sein. Ein neues Tokenverbot beendet zudem keine bereits an eine Warteschlange übergebene Verarbeitung; deren Zustand ist separat zu erheben. [Q15, Tokenrevocation; eigene Ableitung zur Anwendungsausführung]

4. Notbetrieb mit realer Personal- und Kommunikationsgrenze

Im Beispiel kann die Primärbefundung außerhalb des KI-Dienstes weiter erfolgen, sofern die Zuordnung unabhängig überprüfbar bleibt. Das ist die erste zu prüfende Ersatzfähigkeit. Es darf nicht aus dem Vorhandensein eines Ausdrucks geschlossen werden, dass ein durchgängiger Prozess existiert. Der Ausdruck braucht Identität, Zeitpunkt, Version, zuständige Empfänger und eine dokumentierte Kenntnisaufnahme.

Fällt zusätzlich eine Integrationskomponente aus, steigen manuelle Aufgaben. Die fachliche Leitung legt fest, welche Leistung mit vorhandenem Personal über welchen Zeitraum erbracht werden kann und wann Kapazität eingeschränkt oder externe Unterstützung benötigt wird. Eine Liste theoretisch verfügbarer Papierformulare ersetzt diese Entscheidung nicht. Klinische Downtime-Leitlinien und Erfahrungsberichte begründen die Bedeutung vorbereiteter Ersatzabläufe, belegen aber nicht die Leistungsfähigkeit dieses fiktiven Betriebs. [Q17; Q18; Q21,

Abstract]

Ein Ausweichen auf „alle Geräte lokal“ wäre insbesondere für Überwachungstechnik nicht automatisch sicher. Bei manchen konkreten Geräten kann das Wegfallen der Vernetzung zusätzliche Anwesenheit am Gerät erfordern. Der FDA-Fall in Q19 illustriert diesen gerätespezifischen Zusammenhang; er ist keine Anweisung, beliebige Patientenmonitore zu trennen.

5. Prüfaufbau und verlangte Evidenz

In einer freigegebenen Testumgebung werden ausschließlich synthetische Patienten- und Auftragskennungen verwendet. P-K01 führt einen gültigen Befund durch den gesamten vorgesehenen Weg. Erwartet werden richtige Zuordnung, erkennbare Version, unveränderte Primärinformation und korrekt begrenzter Entwurfsstatus. P-K02 sendet eine formal gültige, aber widersprüchliche Zuordnung. Erwartet wird ein definierter Klärungszustand statt einer unmarkierten klinischen Ausgabe.

P-K03 widerruft die Dienstberechtigung, während ein Auftrag bereits wartet. Der Test beobachtet nicht nur die Authentifizierungsantwort, sondern auch die spätere Ausführung. P-K04 prüft, ob ein fachlich korrigierter Befund die alte Zusammenfassung erkennbar veraltet und einen erneuten Prüfbedarf auslöst. P-K05 verfolgt einen Ersatzprozess über den Schichtwechsel bis zum späteren Abgleich. Erwartete Evidenz sind zuordenbare Testprotokolle, Systemstände, Ausgaben, Empfangsnachweise und fachliche Bewertungen; im Paket selbst liegen diese lokalen Nachweise nicht vor.

Zuordnung: K09–K18 betreffen den klinischen Pfad, K29–K36 den Agentenzugriff und K52–K60 die Wiederherstellung. E-K01 bis E-K05 sind im Beispielregister nur **erforderliche Nachweisobjekte**. Ihr Status bleibt NICHT_ERHOBEN.

6. Wiederherstellung und Zusammenführung

Die Freigabe einer technisch bereinigten Integration beantwortet noch nicht, welche inzwischen entstandenen Informationen gültig sind. F11 führt deshalb alle betroffenen Aufträge, Entwürfe, Korrekturen und manuellen Ereignisse mit ihrem jeweiligen Status zusammen. Eine Originalinformation bleibt mit ihrer Änderungs Historie nachvollziehbar. Eine doppelte Nachricht darf nicht zu einem zusätzlichen klinischen Vorgang führen. Ein ungeklärter Widerspruch wird nicht durch automatisches „neuester Datensatz gewinnt“ aufgelöst.

Der technische Wiederanlauf wird auf einen begrenzten Funktionsumfang beschränkt. Die fachliche Freigabe der Datenzuordnung ist eine eigene Entscheidung. Der KI-Dienst erhält erst danach die konkret benötigten Rechte zurück. Die Wiederaufnahme ist widerrufbar; erhöhte Beobachtung, zuständige Rückfallebene und Abbruchkriterien stehen in F10 und F16.

7. Ausschussentscheidung und verbleibende Unsicherheit

Eine geeignete Entscheidung wäre konditional: „Der betrachtete Zusammenfassungspfad kann nach belegter Zuordnungsprüfung und abgeglichenen betroffenen Fällen eingeschränkt wieder aufgenommen werden; automatische Übernahme in fachlich verbindliche Dokumentation bleibt ausgeschlossen.“ Diese Formulierung beschreibt eine mögliche Entscheidung nach erfolgreicher lokaler Prüfung, nicht den aktuellen Status eines realen Systems.

Offen bleiben unter anderem unentdeckte alternative Datenpfade, Personalengpässe im verlängerten Notbetrieb und die Qualität außerhalb des geprüften Fallraums. Ein Ausschuss sollte deshalb fragen, welche Gegenprobe die Freigabe aufheben würde, wer neue Befundwidersprüche bewertet und wann der Ersatzbetrieb seine Kapazitätsgrenze erreicht. Sind Identitäten oder Primärbefunde breiter kompromittiert als angenommen, ist der ursprüngliche begrenzte Scope nicht mehr tragfähig.

S-INDUSTRIE · Der Roboter stoppt sicher, die produzierte Charge ist trotzdem zweifelhaft

1. Auftrag und Annahmen

Ein fiktiver Fertigungsbereich verbindet Produktionsplanung, Rezeptverwaltung, Roboterzellen und eine Flotte autonomer Transportfahrzeuge. Ein Optimierungsagent darf Vorschläge für die Auftragsreihenfolge erstellen. Ein zeitweise freigeschalteter Wartungsdienst darf Diagnosen an einer bestimmten Zelle durchführen. Lokale Schutzfunktionen begrenzen die Maschinenbewegung unabhängig von der normalen Aufgabenplanung. Ob diese Unabhängigkeit tatsächlich besteht, ist im realen Einsatz zu prüfen; das Beispiel setzt sie nicht als bewiesene Eigenschaft voraus. [Q02, §§ 2.3.7, 5.2–5.3; Q24, öffentlicher Scope]

Angenommen wird ein Berechtigungsfehler: Der Wartungszugang kann auch eine zentrale Rezeptdatei verändern. Das ist für seinen Auftrag unnötig. Ein bereits zugestellter Fertigungsauftrag verweist nur auf den Namen des Rezepts und bindet keine konkrete freigegebene Version. Damit entsteht eine mögliche Wirkungskette, obwohl keine Safety-Grenze geändert wird.

2. Warum eine reine Safety-Betrachtung zu kurz greift

Eine erfolgreiche Schutzabschaltung wäre in diesem Fall wertvoll, würde aber die Integrität zuvor gefertigter Teile nicht beweisen. Produktqualität, Nachverfolgbarkeit und mechanische Gefährdung sind unterschiedliche Prüfgegenstände. Umgekehrt bedeutet eine unzulässige Rezeptänderung nicht automatisch, dass jede Maschine eine Person gefährdet. Diese Differenzierung verhindert sowohl Entwarnung als auch Übertreibung.

Das Risikoregister trennt deshalb R-I01 „nicht freigegebene Rezeptversion wird verwendet“, R-I02 „nach Widerruf wird ein alter Auftrag ausgeführt“ und R-I03 „Eingrenzung unterbricht einen für sicheren Anlagenzustand erforderlichen Hilfsprozess“. Der dritte Pfad entsteht erst durch die Abwehrreaktion und muss trotzdem im Voraus betrachtet werden. Die konkrete sichere Reaktion hängt von Anlage, Material, Energie und Prozess ab; „Strom aus“ ist keine allgemeine Lösung. [Q02, OT-Charakteristika und Verfügbarkeit/Safety]

3. Eingrenzung nach Funktionen statt pauschalem Netzwerkbild

Der Wartungszugang verliert zunächst die nicht erforderliche Schreibmöglichkeit. Zugleich werden verdächtige Rezeptänderungen und ihre Verwendung erhoben. Eine Sperre des zentralen Kontos genügt nicht, wenn eine lokal zwischengespeicherte Berechtigung oder ein bereits angenommenes Kommando weiterwirkt. Flottenmanager, Zellensteuerung und Auftragswarteschlange müssen daher getrennt betrachtet werden.

Die Produktionsverantwortlichen entscheiden, welche Aufträge weitergeführt, kontrolliert angehalten oder nicht neu gestartet werden. Maßgeblich sind die anlagenspezifische Gefährdungsbeurteilung und die validierten Betriebsarten. Das Security-Team besitzt nicht automatisch das Mandat, die Energieversorgung eines unbekannten Prozesses zu unterbrechen. Hersteller oder Integrator werden hinzugezogen, soweit die sichere Durchführung oder die Beurteilung des Konfigurationsstands dies erfordern.

Die Qualitätssicherung grenzt betroffene Produkte anhand von Versionsverwendung, Prozesszeitraum und Rückverfolgbarkeit ein. Ein bloßer Kalenderbereich reicht nicht, wenn verschiedene Zellen Rezeptänderungen unterschiedlich übernehmen. Die Entscheidung über Produktfreigabe bleibt von der Freigabe des Netzwerks getrennt.

4. Die entscheidenden technischen Gegenproben

P-I01 prüft, ob ein Auftrag an eine bestimmte freigegebene Rezeptversion gebunden ist. Der Positivfall verwendet eine gültige Kombination. Der Negativfall verändert nach der fachlichen Freigabe die referenzierte Version beziehungsweise versucht eine veraltete Version erneut zu verwenden. Erwartet wird eine erneute Prüfung oder Ablehnung nach dem lokalen Entwurf, nicht die stillschweigende Ausführung eines beliebigen aktuellen Dateiinhalts.

P-I02 widerruft den Wartungszugang und beobachtet neue, bereits angenommene und zwischengespeicherte Anforderungen getrennt. P-I03 simuliert im freigegebenen Testaufbau eine unerwartete Flottenmission. Die Simulation prüft die Auftragsberechtigung und die definierten Zustandsübergänge; sie fährt nicht absichtlich eine gefährliche Bewegung im laufenden Betrieb.

P-I04 untersucht die angenommene Unabhängigkeit der lokalen Schutzfunktion. Dazu gehören Konfiguration, administrative Zugänge und gemeinsame Abhängigkeiten. Der Test ist durch fachkundige Safety-Verantwortliche festzulegen. Er darf nicht mit einem improvisierten Angriff auf eine produktive Sicherheitssteuerung verwechselt

werden. Öffentliche Metadaten zu ISO 10218 und IEC 62443 ersetzen weder die relevanten Normvolltexte noch die konkrete Validierung. [Q24–Q26, jeweils Scope/Metadaten]

5. Wiederaufbau und Produktentscheidung

Die Wiederherstellung umfasst freigegebene Engineering-Stände, Rezeptversionen, Roboterprogramme, relevante Berechtigungen und die reale Anlagenlage. Ein gespeicherter Flottenzustand kann falsch sein, wenn Fahrzeuge oder Ladungsträger im Notbetrieb bewegt wurden. Ein digital korrektes Abbild ist nur dann brauchbar, wenn es den tatsächlich erhobenen Zustand repräsentiert.

F10 dokumentiert, welche technische Funktion unter welchen Bedingungen zurückkehrt. F11 dokumentiert separat die Zuordnung von Material, Zwischenprodukten und fertigen Einheiten zu gültigen Prozessinformationen. Ein Systembackup kann diese fachliche Rekonstruktion unterstützen, aber nicht ersetzen. NISTs OT-Backup-Leitfaden ist hierfür eine Grundlage zur Einbeziehung der benötigten Betriebs- und Engineering-Informationen. [Q08, Leitfadenbeschreibung]

Die Rückkehr in den Betrieb erfolgt nicht durch Wiedervergabe aller früheren Rechte. Der Ausgangsfehler wird beseitigt: Diagnosezugriff bleibt auf den vereinbarten Scope beschränkt; Aufträge werden ausreichend an freigegebene Zustände gebunden; Lieferantenrechte laufen aus und sind nachvollziehbar. K19–K28, K30–K36 und K52–K60 bilden die relevanten Kontrollen ab.

6. Mögliche Freigabe und Gegenbeleg

Ein geeignetes Prüfergebnis könnte die Steuerungsfunktion freigeben, während die Produktfreigabe für einen abgegrenzten Bestand offen bleibt. Das ist kein Widerspruch, sondern Ausdruck getrennter Schutzgegenstände. Ebenso kann ein Teilbereich mit validiertem lokalen Betrieb weiterarbeiten, während die zentrale Optimierung deaktiviert bleibt.

Die Freigabe scheitert, wenn die verwendeten Rezeptstände nicht rekonstruierbar sind, ein nicht erfasster Administrationspfad weiterbesteht oder die angenommene sichere Betriebsart nicht nachgewiesen werden kann. Ein pauschales „Backup eingespielt, Anlage grün“ wäre unzureichend. Die Prüfsache muss klar erkennen lassen, welcher Funktionsumfang, welcher Produktbestand und welche Restunsicherheit von der Entscheidung umfasst sind.

S-ABWEHR · Ein plausibler Fehlalarm darf nicht die gesamte Organisation abschalten

1. Auftrag und konkurrierende Risiken

Ein fiktiver Sicherheitsdienst beobachtet ungewöhnliche Datenzugriffe. Ein defensiver Agent darf Meldungen anreichern, eng begrenzte Tokens sperren und innerhalb eines vorab genehmigten Mandats einzelne Ausleitungspfade einschränken. Er darf keinen gemeinsamen Identitätsdienst oder alle medizinischen beziehungsweise industriellen Netze selbstständig abschalten. Diese Grenze ist eine vorgeschlagene Architekturentscheidung, keine allgemeine gesetzliche Pflichtformulierung.

Das Beispiel beginnt mit einem genehmigten Migrationslauf, dessen Zugriffsmuster von der Normalverteilung abweicht. Gleichzeitig enthält ein aus einer Anwendung übernommener Logtext eine Anweisung, „zur Sicherheit“ weitere Konten zu sperren. Der Text wird als potenziell manipulierte Beobachtung behandelt, nicht als Handlungsbefehl. Die Sicherheitsprüfung muss sowohl einen echten Datenabfluss als auch eine selbst verursachte Betriebsstörung vermeiden. [Q11, Taxonomie bösartiger Eingaben; Q05, Incident Response; Q10, Identitätsgrundlagen]

2. Was die Erkennung wissen darf – und was nicht

Eine fachlich legitime Ausnahme darf nicht nur durch den untersuchten Agenten selbst bestätigt werden. Für das Migrationsfenster braucht es einen getrennten, zuständigen Nachweis von Auftrag, Datenscope und Zeitraum. Der Sicherheitsdienst prüft, ob die beobachtete Handlung dazu passt. Eine beliebige Zeichenfolge „approved“ im Log oder in einem Tickettext ist kein ausreichender Beleg.

Die Entscheidung berücksichtigt unvollständige Daten. Fehlt die Auftragsinformation, beweist das weder einen Angriff noch die Zulässigkeit des Zugriffs. Das System kann zunächst die risikoreiche neue Ausleitung begrenzen und eskalieren, statt alle abhängigen Dienste abzuschalten. Welche Aktion tatsächlich angemessen ist, muss aus den lokalen Folgen beider Alternativen abgeleitet werden. Die Formulierung „im Zweifel immer trennen“ wäre bei kritischen gemeinsamen Diensten zu grob.

3. Reaktionsmandat und menschliche Entscheidung

F09 legt für jede automatische Reaktion Auslöser, zulässigen Umfang, Zeitgrenze, Rücknahme und erforderliche fachliche Beteiligung fest. Für einen begrenzten, wiederholbaren Zugriff kann eine automatische Einschränkung zugelassen werden. Eine organisationsweite Änderung der Identitätsinfrastruktur verlangt eine andere Entscheidungsebene und einen belegten Notbetrieb.

Die menschliche Freigabe erhält den beobachteten Zugriff, den betroffenen Auftrag, die mögliche Schadensfolge, die vorgeschlagene Reaktion und deren Auswirkungen. Eine Meldung „KI empfiehlt Sperre, bestätigen?“ ist nicht ausreichend. Das Beispiel prüft ausdrücklich auch Vertretung und Reaktionsfähigkeit außerhalb der Regelarbeitszeit. Steht kein entscheidungsfähiger Mensch rechtzeitig zur Verfügung, muss vorher geregelt sein, welcher begrenzte Ersatzmodus gilt. Ein unrealistischer Human-in-the-Loop ist keine Schutzbarriere.

4. Drei Prüfungen statt einer beeindruckenden Demonstration

P-A01 prüft einen echten, im Test synthetisch erzeugten unzulässigen Ausleitungspfad und erwartet die mandatsgemäße Einschränkung. P-A02 prüft den legitimen Migrationslauf und erwartet eine nachvollziehbare Bewertung ohne ungerechtfertigte organisationsweite Abschaltung. P-A03 legt eine manipulative Handlungsanweisung als Loginhalt vor und erwartet, dass daraus keine neue Berechtigung oder Reaktion entsteht.

Das Testdesign variiert die Verfügbarkeit des Freigabenachweises und die Datenlage. Es prüft außerdem, ob der defensive Agent sein eigenes Mandat ändern kann, ob Reaktionen mehrfach ausgelöst werden und ob ein Widerruf die tatsächliche Fortsetzung verhindert. Relevante Kontrollen sind K03, K29–K38 sowie K49–K60. Die Ergebnisfelder bleiben bis zur Ausführung offen.

Ein einzelner bestandener Angriffstest sagt wenig über die Anzahl der Fehlalarme im Normalbetrieb. Daher werden Grundgesamtheit, getestete Varianten, Treffer, Fehlalarme, Nichterkennungen und Entscheidungszeiten separat erfasst. Die mathematischen Beispiele in L06 illustrieren diesen Unterschied; sie sind keine Leistungsangaben eines realen Produkts.

5. Ausschussentscheidung und Restrisiko

Eine mögliche begrenzte Freigabe erlaubt dem Agenten Anreicherung und eng definierte reversible Reaktionen, nicht aber neue organisationsweite Kontrollrechte. Der Ausschuss verlangt Nachweise sowohl für Angriffsabwehr als auch für Fehlalarmbeherrschung. Fehlen diese, kann der Dienst zunächst nur beobachtend eingesetzt werden; dies muss wiederum zu den lokalen Schutzanforderungen passen.

Das verbleibende Risiko ist nicht Null. Ein engeres Mandat kann einen Angriff später eindämmen; ein breiteres kann legitimen Betrieb treffen. Die Aufgabe besteht darin, den zulässigen Handlungsspielraum anhand von Schutzbedarf, Reaktionszeit und Ersatzfähigkeit zu begründen. Diese Entscheidung muss bei neuen Modellen, Werkzeugen, Datenquellen oder Betriebsabhängigkeiten erneut geprüft werden.

Gemeinsame Auswertung

Alle drei Fälle widerlegen dieselben Kurzschlüsse: technischer Zugang ist nicht fachliche Erlaubnis; verfügbare Daten sind nicht notwendigerweise vertrauenswürdig; ein widerrufenes Token beendet nicht jede bereits ausgelöste Wirkung; erfolgreiche Wiederherstellung ist nicht automatisch fachliche Freigabe. Ebenso wenig lässt sich jede Abhängigkeit durch einen globalen Not-Aus sinnvoll beherrschen.

Der praktische Abschluss ist jeweils eine **begrenzte, begründete und widerrufbare Entscheidung mit auffindbaren Nachweisen**. Das Beispielregister zeigt die Struktur; erst örtliche Erhebung, freigegebene Tests, fachliche Bewertung und dokumentierte Restrisikoentscheidung machen daraus eine tatsächlich nutzbare Betriebsfreigabe.

Quellen- und Navigationshinweis

Die vollständigen Angaben und Zugriffsbeschränkungen zu sämtlichen Q-Nummern stehen in 03_QUELLEN/QUELLENREGISTER.md. Die Fallkonstruktionen sind keine zusätzlichen empirischen Quellen. Zur direkten Anwendung: L02 für S-KLINIK; L03 für S-INDUSTRIE; L04 und L06 für S-ABWEHR; L05 für die Entscheidung und die lokale Rechtsanwendbarkeit.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.